

## 内 容 简 介

本书是作者在几所大学授课时所使用讲义的基础上,经多次修改和补充而成。全书共分五章:第一章域的扩张,第二章代数扩张,第三章 Galois 理论,第四章超越扩张,第五章整扩张。作者在题材的选择和安排上,着眼于域的基本理论和基本方法以及对于其他学科应用较多的内容,给只具有高等代数及抽象代数初步知识的读者提供了一本系统地学习域论基础的书。

本书可做大学数学系学生的教材或教参。

## 序

域是代数学中最基本的概念之一，历史悠久。早在十九世纪初叶，在 Galois 研究方程的著作中就有了域的概念的萌芽，虽然那时还没有域的抽象定义。1910年，Ernst Steinitz的论文《体的代数理论》，(Algebraische Theorie der Körper, J. reine und angew. Math. 137 (1910))问世。在这篇论文里，第一次对于域的理论作了全面、系统的阐述，奠定了域论的基础。时至今日，域论不仅本身是代数学中一个内容丰富的重要分支，而且也是学习其它一些分支，如代数数论，代数几何，环论，代数群等所不可缺少的基础知识，此外，有限域在近代的编码和计算机理论中都有着应用。

这本书最初是作者于1982年春应云南大学数学系之邀，在该系讲授域论时所编写的讲义，以后又经过多次修改和补充。共包括五章。第一章介绍域扩张及有关的一些最基本的概念，这是研究域的基本思想；第二章介绍代数扩张，其中对于可分性的问题作了较细致的讨论；第三章介绍 Galois 理论；第四章介绍超越扩张，包括超越基及超越次数，可分性，导子等；第五章介绍整扩张，包括环的整扩张，局部化及 Hilbert 零点定理等，这是交换代数的最基本的内容，有着广泛的应用。作者的意图是向只具有高等代数及抽象代数初步知识的读者提供一本系统地介绍域论基础的书。在题材的选择和安排上，着眼于域的基本理论和基本方法以及对于其它学科应用较多的内容，并不追求全面和完备，因此，对于有些本来应该属于域论的题材，如有序域，赋值等，就没有包括进去。

首先要感谢云南大学数学系的一些同事，正是由于他们的盛情邀请，才使作者想到要编写一本有关域方面的书。在编写过程中，我的许多同事曾给予不少帮助。特别是蒋滋梅同志，她不仅仔细地阅读了原稿，而且还用原稿作为讲义，在本校及外校讲授了数次，提出了很多宝贵的意见。谨在这里表示感谢。

希望读者批评指正。

郝柄新

1985年12月于

北京师范大学数学系

# 目 录

第一章 域的扩张 .....	( 1 )
1.1 子域和扩域 添加 .....	( 1 )
1.2 素域 .....	( 4 )
1.3 单扩域 .....	( 6 )
第二章 代数扩紧 .....	( 12 )
2.1 代数扩域 .....	( 12 )
2.2 代数闭包 .....	( 18 )
2.3 正规扩域 多项式的分裂域 .....	( 24 )
2.4 有限域 .....	( 32 )
2.5 可分多项式和不可分多项式 .....	( 38 )
2.6 共轭映射的个数 .....	( 43 )
2.7 可分扩域和不可分扩域 .....	( 46 )
2.8 纯不可分扩域 可分次数和不可分次数 .....	( 53 )
2.9 完备域 .....	( 57 )
2.10 本原元素定理 .....	( 59 )
第三章 Galois理论 .....	( 66 )
3.1 Galois扩域 .....	( 66 )
3.2 一些例子 .....	( 76 )
3.3 基本定理 .....	( 80 )
3.4 单位根 .....	( 88 )
3.5 分圆扩域 .....	( 96 )
3.6 范和迹 .....	( 101 )
3.7 循环扩域 .....	( 107 )



3.8	关于有限群的若干结果 .....	(114)
3.9	可解扩域和根号扩域 .....	(120)
3.10	代数方程的根号解 .....	(125)
3.11	$n$ 次一般方程 .....	(128)
3.12	二次、三次和四次方程 .....	(134)
第四章	超越扩张 .....	(138)
4.1	超越基 超越次数 .....	(138)
4.2	Luroth 定理 .....	(148)
4.3	线性无缘 .....	(152)
4.4	域的代数无关性 .....	(157)
4.5	可分扩张 .....	(161)
4.6	可分生成的扩域 .....	(167)
4.7	导子 .....	(171)
第五章	整扩张 .....	(188)
5.1	模 .....	(188)
5.2	Noether 环 .....	(192)
5.3	交换环的一些理想 .....	(199)
5.4	局部化 .....	(202)
5.5	整扩张 .....	(207)
5.6	整扩张与素理想 .....	(212)
5.7	Noether 的正规化定理 .....	(215)
5.8	代数簇 Hilbert 零点定理 .....	(219)
附 录	.....	(228)
名词索引	.....	(231)

# 第一章 域的扩张

## 1.1 子域和扩域 添加

读者都已熟悉域的定义。一个域是一个至少有两个元素的集  $F$ ，在其中定义了两个代数运算，分别叫做加法和乘法； $F$  对于加法来说作成是一个 Abel 群， $F$  的全体非零元素对于乘法来说作成是一个 Abel 群，并且加法与乘法被分配律联系着。

设  $F$  是域  $K$  的一个子集。如果对于  $K$  的加法和乘法来说， $F$  本身也作成是一个域，就称  $F$  是  $K$  的一个子域，而  $K$  是  $F$  的一个扩域，以后我们常常用符号  $K/F$  表示  $K$  是  $F$  的扩域，并且称为一个域扩张。

设  $K/F$  是一个域扩张。如果  $E$  是  $K$  的一个子域，同时又是  $F$  的一个扩域，就称  $E$  是域扩张  $K/F$  的一个中间域。

设  $F$  是域  $K$  的一个子域。 $T$  是  $K$  的一个子集。令  $\{E_\alpha\}_{\alpha \in I}$  ( $I$  是一个指标集) 是域扩张  $K/F$  中包含  $T$  的中间域的全体。显然， $K \in \{E_\alpha\}_{\alpha \in I}$ ，所以  $\{E_\alpha\}_{\alpha \in I} \neq \emptyset$ 。令  $E = \bigcap_{\alpha \in I} E_\alpha$ 。那么  $E$  是

$K/F$  的一个中间域。它是  $K$  中包含  $F$  和  $T$  的最小子域，记作  $F(T)$ 。称为添加  $T$  于  $F$  所得的扩域，或称为  $T$  在  $F$  上所生成的域。

当  $T = \{t_1, \dots, t_n\}$  是  $K$  的一个有限子集时，我们把  $F(T)$  记作  $F(t_1, \dots, t_n)$ 。这时就说  $F(t_1, \dots, t_n)$  是在  $F$  上有限生成的。特别，添加单独一个元素  $t$  于  $F$  所得的扩域  $F(t)$  叫做  $F$  的一个单扩域。

**定理 1.1.1** 设  $F$  是域  $K$  的一个子域， $T, T_1, T_2$  都是  $K$

的子集。

$$(i) \quad F(T_1 \cup T_2) = F(T_1)(T_2)$$

(ii) 令  $\{S_\alpha\}_{\alpha \in I}$  是  $T$  的一切有限子集所成的子集族。那么

$$F(T) = \bigcup_{\alpha \in I} F(S_\alpha)$$

(iii) 设  $T = \{t_1, \dots, t_n\}$  是有限集。那么

$$F(T) = \left\{ \frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)} \mid f, g \in F[X_1, \dots, X_n], \right. \\ \left. g(t_1, \dots, t_n) \neq 0 \right\}.$$

这里  $F[X_1, \dots, X_n]$  是  $F$  上不相关不定元  $X_1, \dots, X_n$  的多项式环。

证 (i)  $F \subseteq F(T_1)(T_2)$ ,  $T_1 \cup T_2 \subseteq F(T_1)(T_2)$ , 而  $F(T_1 \cup T_2)$  是  $K$  的既包含  $F$  又包含  $T_1 \cup T_2$  的最小子域, 所以

$$F(T_1 \cup T_2) \subseteq F(T_1)(T_2).$$

反过来,  $F(T_1)$  是  $F(T_1 \cup T_2)$  的子域, 又  $T_2 \subseteq F(T_1 \cup T_2)$ . 因为  $F(T_1)(T_2)$  是  $K$  的既包含  $F(T_1)$  又包含  $T_2$  的最小子域, 所以

$$F(T_1)(T_2) \subseteq F(T_1 \cup T_2).$$

(ii) 由定义, 对于每一个  $\alpha \in I$ ,  $F(S_\alpha) \subseteq F(T)$ , 从而  $\bigcup_{\alpha \in I} F(S_\alpha) \subseteq F(T)$ .

令  $L = \bigcup_{\alpha \in I} F(S_\alpha)$ .  $L$  是  $K$  的一个子域. 事实上, 设  $u, v \in L$ , 那么存在  $T$  的有限子集  $S_1$  和  $S_2$ , 使得  $u \in F(S_1)$ ,  $v \in F(S_2)$ . 令  $S = S_1 \cup S_2$ , 则  $S$  也是  $T$  的有限子集, 并且  $u, v \in F(S)$ . 由于  $F(S)$  是子域, 所以  $u+v$ ,  $u-v$ ,  $uv$ ,  $uv^{-1}$  (若  $v \neq 0$ ) 都属于  $F(S) \subseteq L$ . 这就证明了  $L$  是  $K$  的子域.

现在设  $t \in T$ , 那么  $t \in F(t) \subseteq L$ . 因此  $T \subseteq L$  又  $F \subseteq L$ . 所以  $F(T) \subseteq L$ . 这样,

$$L = \bigcup_{a \in I} F(S_a) = F(T).$$

(iii)  $F$  的元素与  $t_1, \dots, t_n$  经过加、减、乘、除运算的结果都可以表示成以下形状

$$(1) \quad \frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)}, \quad g(t_1, \dots, t_n) \neq 0,$$

这里  $f, g \in F[X_1, \dots, X_n]$ . 这样的元素都属于  $F(t_1, \dots, t_n)$ . 另一方面,  $K$  中一切形如(1)的元素已经作成一个既包含  $F$  又包含  $t_1, \dots, t_n$  的子域. 这就证明了(iii)成立. ■

域  $F$  的扩域  $K$  可以看成  $F$  上一个向量空间. 如果  $K$  在  $F$  上的维数是有限的, 那么就称  $K$  是  $F$  的一个有限次扩域或者称  $K/F$  是一个有限次扩域. 如果  $K$  是  $F$  上无限维的向量空间, 就称  $K$  是  $F$  的一个无限次扩域, 相应地, 称  $K/F$  是一个无限次扩张. 作为向量空间,  $K$  在  $F$  上的维数叫做  $K$  在  $F$  上的次数, 记作  $[K:F]$ , 向量空间  $K$  在  $F$  上的基也称为域  $K$  在  $F$  上的基.

**定理 1.1.2** 设  $E$  是域扩张  $K/F$  的一个中间域.  $\{u_\alpha\}_{\alpha \in I}$  是  $E$  在  $F$  上的一个基而  $\{v_\beta\}_{\beta \in J}$  是  $K$  在  $E$  上的一个基. 那么  $\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$  是  $K$  在  $F$  上的一个基.

**证** 首先  $\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$  里任意有限个元素  $\{u_i v_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$  在  $F$  上线性无关. 事实上, 如果有  $a_{ij} \in F$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq n$ , 使得

$$\sum_{i=1}^m \sum_{j=1}^n a_{ij} u_i v_j = 0,$$

则

$$\sum_{j=1}^n \left( \sum_{i=1}^m a_{ij} u_i \right) v_j = 0.$$

$\sum_{i=1}^m a_{ij} u_i \in E$ ,  $1 \leq j \leq n$ , 而  $v_1, \dots, v_n$  在  $E$  上线性无关, 所以

$$\sum_{i=1}^m a_{ij} u_i = 0, \quad 1 \leq j \leq n.$$

又因为  $u_1, \dots, u_m$  在  $F$  上线性无关, 所以  $a_{ij} = 0, \quad 1 \leq i \leq m, 1 \leq j \leq n$ .

其次, 设  $u \in K$ , 那么  $u$  可以由  $\{u_\beta\}_{\beta \in J}$  中有限个元素  $v_1, \dots, v_n$  线性表示, 系数属于  $E$ :

$$u = \sum_{j=1}^n b_j v_j, \quad b_j \in E \quad (1 \leq j \leq n).$$

每一个  $b_j$  又可以表成  $\{u_\alpha\}_{\alpha \in I}$  中有限元素的  $F$ -线性组合. 因此存在  $u_1, \dots, u_m \in \{u_\alpha\}_{\alpha \in I}$ , 使得

$$b_j = \sum_{i=1}^m a_{ij} u_i, \quad a_{ij} \in F \quad (1 \leq i \leq m, 1 \leq j \leq n).$$

于是

$$u = \sum_{i=1}^m \sum_{j=1}^n a_{ij} u_i v_j.$$

所以  $u$  可以表成  $\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$  中有限个元素的  $F$ -线性组合. 这就证明了  $\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$  是  $K$  在  $F$  上的一个基. ■

由这个定理, 我们立即得到以下

**推论 1.1.3** 设  $K/F$  是一个有限次域扩张, 而

$$E_1 \subseteq E_2 \subseteq \dots \subseteq E_s$$

都是  $K/F$  的中间域. 那么

$$[K : F] = [K : E_s][E_s : E_{s-1}] \cdots [E_1 : F]. \quad \blacksquare$$

## 1.2 素域

如果一个域没有真子域, 就称为一个素域.

有理数域  $\mathbb{Q}$  显然是一个素域. 设  $\mathbb{Z}$  是整数环,  $p$  是一个素数. 令

$$(p) = \{pn \mid n \in \mathbb{Z}\}$$

是  $p$  所生成的  $\mathbb{Z}$  的理想. 我们知道, 以  $p$  为模的剩余类环  $\mathbb{Z}/(p)$  是一个域并且也是素域.

下面的定理对素域作了完全的描述.

**定理 1.2.1** 令  $F$  是一个素域. 那么  $F$  或者与有理数域  $\mathbb{Q}$  同构, 或者与以某一个素数  $p$  为模的剩余类环同构.

**证** 令  $1$  是素域  $F$  的单位元, 映射

$$\varphi: \mathbb{Z} \rightarrow F, \quad n \rightarrow n \cdot 1$$

是一个环同态. 令  $\mathfrak{p} = \ker \varphi$  是  $\varphi$  的核. 则  $\mathfrak{p}$  是  $\mathbb{Z}$  的一个理想, 且

$$\mathbb{Z}/\mathfrak{p} \cong \varphi(\mathbb{Z}) \subseteq F.$$

因为  $\varphi(1) \neq 0$ , 所以  $\mathfrak{p} \neq \mathbb{Z}$ . 由于  $\varphi(\mathbb{Z})$  是整环, 而  $\mathbb{Z}$  是主理想环, 因此, 或者  $\mathfrak{p} = (0)$ , 或者  $\mathfrak{p} = (p)$ , 这里  $(p)$  是由某一个素数  $p$  所生成的  $\mathbb{Z}$  的理想.

如果  $\mathfrak{p} = (0)$ , 那么  $\varphi$  是单射, 并且可以开拓为  $\mathbb{Z}$  的商域  $\mathbb{Q}$  到  $F$  的单射,  $\varphi(\mathbb{Q})$  是  $F$  的子域. 因为  $F$  是素域, 所以  $\varphi(\mathbb{Q}) = F$ . 这样,  $\mathbb{Q} \cong F$ .

如果  $\mathfrak{p} = (p)$ , 那么  $\mathbb{Z}/\mathfrak{p} = \mathbb{Z}/(p)$  是域, 从而  $\varphi(\mathbb{Z})$  是  $F$  的子域. 因为  $F$  是素域, 所以  $\varphi(\mathbb{Z}) = F$ , 这样就得到  $\mathbb{Z}/(p) \cong F$ . ■

设  $F$  是任意一个域.  $F$  的一切子域的交  $F_0$  仍是  $F$  的一个子域.  $F_0$  显然是  $F$  的最小子域, 所以  $F_0$  是一个素域, 称为域  $F$  的素域. 由 1.2.1 知, 或者  $F_0 \cong \mathbb{Q}$ , 或者  $F_0 \cong \mathbb{Z}/(p)$ ,  $p$  是一个素数. 在前一情形, 就说  $F$  具有特征零; 在后一情形, 就说  $F$  具有特征  $p$ . 我们把域  $F$  的特征记作  $\text{char } F$ . 下面两个定理是比较显易的, 我们把它们的证明留给读者去作.

**定理 1.2.2** 设  $F$  是一个域.

(i) 如果  $\text{char } F = 0$ , 那么对于  $n \in \mathbb{Z}$ ,  $x \in F$ ,

$$nx = 0 \iff x = 0 \text{ 或 } n = 0.$$

(ii) 如果  $\text{char } F = p > 0$ , 那么对于  $n \in \mathbb{Z}$ ,  $x \in F$ ,

$$nx = 0 \iff x = 0 \text{ 或 } n \equiv 0 \pmod{p}. \quad \blacksquare$$

**定理 1.2.3** 设  $F$  是一个域,  $\text{char } F = p > 0$ . 那么对于任意  $x, y \in F$  和任意非负整数  $n$ ,

$$(i) \quad (x \pm y)^{p^n} = x^{p^n} + y^{p^n};$$

(ii) 映射  $\varphi: x \mapsto x^{p^n}$  是  $F$  到自身内的同态单射. ■

### 1.3 单扩域

设  $F$  是一个域, 添加一个元素  $\alpha$  于  $F$  所得的扩域  $F(\alpha)$  叫做  $F$  的一个单扩域.

单扩域的结构和所添加的元素  $\alpha$  的性质有着密切的关系, 先引入以下的概念.

设  $R$  是一个有单位元 1 的交换环,  $F$  是  $R$  的一个子域且  $F$  含有  $R$  的单位元.  $R$  的一个元素  $\alpha$  称为关于  $F$  是代数的或者说  $\alpha$  是  $F$  上一个代数元, 如果存在  $F$  上一个非零多项式  $f(X)$ , 使得  $f(\alpha) = 0$ , 如果  $\alpha$  不是  $F$  上的代数元, 就称  $\alpha$  关于  $F$  是超越的或者说  $\alpha$  是  $F$  上一个超越元.

设  $K$  是  $R$  的一个子域, 且  $F \subseteq K$ . 如果  $\alpha \in R$  关于  $F$  是代数的, 那么显然  $\alpha$  关于  $K$  也是代数的. 一个等价的提法是, 如果  $\alpha$  关于  $K$  是超越的, 那么  $\alpha$  关于  $F$  也是超越的.

单扩域的结构由下面的定理完全决定.

**定理 1.3.1** 设  $K = F(\alpha)$  是域  $F$  的一个单扩域.

(i) 如果  $\alpha$  关于  $F$  是超越的, 那么  $K$  与  $F$  上不定元  $X$  的有理分式域  $F(X)$  同构.

(ii) 如果  $\alpha$  关于  $F$  是代数的, 那么存在  $F$  上一个最高次项系数是 1 的不可约多项式  $p(X)$ . 而  $K$  与剩余类环  $F[X]/(p(X))$  同构, 这里  $(p(X))$  表示由多项式  $p(X)$  所生的  $F[X]$  的理想; 这个多项式  $p(X)$  由  $\alpha$  唯一确定.

**证** 对于每一个  $f(X) \in F[X]$ , 令  $f(\alpha) \in K$  与它对应, 这

样就定义了一个环同态  $\varphi: F[X] \rightarrow K$ , 并且  $\varphi$  保持  $F$  的元素不动.  $\varphi(F[X]) = F[\alpha]$  是  $K$  的一个子整环. 令

$$\mathfrak{p} = \text{Ker } \varphi = \{f(X) | f(X) \in F[X], f(\alpha) = 0\}.$$

$\mathfrak{p}$  是环  $F[X]$  的一个理想.

(i) 如果  $\alpha$  关于  $F$  是超越的, 那么不存在非零多项式  $f(X) \in F[X]$  使  $f(\alpha) = 0$ , 从而  $\mathfrak{p} = (0)$ . 所以  $\varphi$  是  $F[X]$  到  $F[\alpha]$  的同构映射, 这个映射可以开拓为有理分式域  $F(X)$  到整环  $F[\alpha]$  的商域  $F(\alpha)$  的同构映射, 仍以  $\varphi$  表示:

$$\varphi: \frac{f(X)}{g(X)} \mapsto \frac{f(\alpha)}{g(\alpha)}.$$

这样,  $\varphi$  是  $F(X)$  到  $K$  同构映射, 且  $\varphi(X) = \alpha$ .

(ii) 设  $\alpha$  关于  $F$  是代数的, 那么存在  $F[X]$  的非零多项式  $f(X)$ , 使得  $f(\alpha) = 0$ , 所以  $\mathfrak{p} \neq (0)$ . 由于  $F[X]$  是欧氏环, 所以  $\mathfrak{p}$  由一个多项式  $p(X) \neq 0$  生成:  $\mathfrak{p} = (p(X))$ ,  $p(X)$  是使  $p(\alpha) = 0$  的非零多项式中次数最低的一个. 不妨设  $p(X)$  的最高次项系数等于 1, 于是  $p(X)$  由  $\alpha$  唯一确定, 并且容易看出,  $p(X)$  是不可约的. 于是  $\mathfrak{p} = (p(X))$  是  $F[X]$  的一个极大理想, 从而剩余类环  $F[X]/\mathfrak{p}$  是一个域, 于是就有

$$F[X]/\mathfrak{p} \cong \varphi(F[X]) = F[\alpha] \subseteq K.$$

因此  $F[\alpha]$  也是域, 然而  $K = F(\alpha)$  是含有  $F$  及  $\alpha$  的最小域, 所以

$$F(\alpha) = F[\alpha], \text{ 即}$$

$$F[X]/\mathfrak{p} \cong K. \quad \blacksquare$$

**定理 1.3.1** 完全给出了一个域  $F$  的单扩域  $F(\alpha)$  的结构, 当  $\alpha$  是  $F$  上的代数元时, 我们还可以说得更具体一些. 首先, 由 1.3.1, 当  $\alpha$  是  $F$  上代数元时, 存在唯一的最高次项系数是 1 的不可约多项式  $p(X) \in F[X]$ , 使得  $p(\alpha) = 0$ . 我们把这个由  $\alpha$  所唯一确定的多项式  $p(X)$  叫做  $\alpha$  在  $F$  上的**最小多项式**. 我们有



**定理 1.3.2** 设  $\alpha$  是域  $F$  上一个代数元,  $p(X) \in F[X]$  是  $\alpha$  在  $F$  上的最小多项式, 设  $\deg p(X) = n$ .

(i) 元素  $1, \alpha, \dots, \alpha^{n-1}$  构成  $F(\alpha)$  在  $F$  上的一个基, 从而  $F(\alpha)$  的每一元素  $\xi$  可以唯一地表示成

$$\xi = a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}, a_i \in F (0 \leq i \leq n-1),$$

的形式.  $[F(\alpha) : F] = \deg p(X)$ .

(ii) 设  $\xi = \sum_{i=0}^{n-1} a_i \alpha^i, \eta = \sum_{i=0}^{n-1} b_i \alpha^i \in F(\alpha)$ , 那么

$$\xi + \eta = \sum_{i=0}^{n-1} (a_i + b_i) \alpha^i$$

(iii) 令  $f(X) = \sum_{i=0}^{n-1} a_i X^i, g(X) = \sum_{i=0}^{n-1} b_i X^i$  而

$$r(X) = c_0 + c_1 X + \dots + c_{n-1} X^{n-1}$$

是以  $p(X)$  除  $f(X)g(X)$  所得的余式, 则

$$\xi \eta = \sum_{i=0}^{n-1} c_i \alpha^i.$$

**证** 由 1.3.1, 对于  $K = F(\alpha) = F[\alpha]$  的任意元素, 存在  $f(X) \in F[X]$ , 使得  $\xi = f(\alpha)$ . 设

$$f(X) = p(X)q(X) + r(X),$$

这里或者  $r(X) = 0$ , 或者  $\deg r(X) < n$ , 那么

$$\xi = f(\alpha) = r(\alpha).$$

因此

$$\xi = a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}, a_i \in F (0 \leq i \leq n-1).$$

这个表示法是最唯一的, 因为如果

$$\xi = \sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} a'_i \alpha^i, a_i, a'_i \in F,$$

那么令  $g(X) = \sum_{i=0}^{n-1} (a_i - a'_i) X^i \in F[X]$ , 则  $g(\alpha) = 0$ , 所以  $p(X)$

整除  $g(X)$ , 从而必须  $g(X) = 0$ , 这样就证明了,  $1, \alpha, \dots, \alpha^{n-1}$  是

$F(\alpha)$  在  $F$  上的一个基, 从而  $[F(\alpha) : F] = n$ . 至于论断 (ii) 和 (iii) 是显然的. ■

由以上两个定理立即得到

**推论 1.3.3** 设  $K = F(\alpha)$  是域  $F$  的一个单扩域.  $K$  是  $F$  上有限次扩域必要且只要  $\alpha$  关于  $F$  是代数的. ■

因为域  $F$  上不定元是存在的, 所以由 1.3.1 (i) 可知, 域  $F$  上添加一个超越元的单扩域是存在的. 下面的定理表明, 域  $F$  上添加一个代数元的单扩也是存在的.

**定理 1.3.4** 设  $p(X) \in F[X]$  是域  $F$  上不定元  $X$  的一个不可约多项式. 那么存在  $F$  的一个扩域  $K$ , 使得  $p(X)$  在  $K$  内有一个根  $\alpha$ , 并且  $K = F(\alpha)$ .

**证** 令  $\mathfrak{p} = (p(X))$  是  $p(X)$  所生成的  $F[X]$  理想. 由于  $p(X)$  不可约, 所以  $\mathfrak{p}$  是一个极大理想. 令  $K = F[X]/\mathfrak{p}$ , 则  $K$  是一个域. 因为  $F \cap \mathfrak{p} = \{0\}$ , 所以自然同态  $\varphi : F[X] \rightarrow K$  将  $F$  单地映入  $K$ , 从而可以将  $\varphi(F)$  与  $F$  等同, 而将  $F$  看成  $K$  的一个子域. 令  $\alpha = \varphi(X) \in K$ , 对于任意  $g(X) \in F[X]$ , 我们有

$$\varphi(g(X)) = g(\varphi(X)) = g(\alpha).$$

所以  $K = \varphi(F[X]) = \{g(\alpha) \mid g(X) \in F[X]\} = F[\alpha]$ , 然而  $K$  是域, 所以  $K = F[\alpha] = F(\alpha)$ . ■

## 习 题

1. 设  $K$  是域  $F$  的一个有限次扩域, 证明:
  - (i)  $[K : F] = 1 \iff K = F$ ;
  - (ii) 如果  $[K : F] = p$  是一个素数, 则在  $F$  与  $K$  之间没有不等于  $F$  或  $K$  的中间域;
  - (iii) 如果  $\alpha \in K$  是  $F$  上一个  $n$  次代数元, 则  $n \mid [K : F]$ .
2. 设  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . 求出  $[K : \mathbb{Q}]$ , 并且给出  $K$  在  $\mathbb{Q}$  上一个基.

3. 设  $F$  是一个素域,  $F(X_1, X_2)$  是  $F$  上不相关不定元  $X_1, X_2$  的有理分式域. 试给出  $F$  的一个扩域  $K$  及  $u, v \in K$ , 使得  $u, v$  都是  $F$  上超越元, 但  $F(u, v) \neq F(X_1, X_2)$ .

4. 证明,  $\mathbb{Q}(\sqrt{2})$  和  $\mathbb{Q}(\sqrt{-1})$  作为  $\mathbb{Q}$  上的向量空间是同构的, 但作为域则不同构.

4. 证明定理 1.2.2. 和 1.2.3.

6. 设  $F(\alpha)$  是域  $F$  上一单扩域. 证明, 如果  $[F(\alpha) : F]$  是一个奇数, 则  $F(\alpha) = F(\alpha^2)$ .

7. 设  $K$  是域  $F$  一个扩域,  $\alpha \in K$ . 证明下列三个条件是等价的:

(i)  $\alpha$  是  $F$  上的代数元;

(ii) 多项式环  $F[\alpha]$  是  $K$  的子域;

(iii)  $F[\alpha]$  是  $F$  上有限维向量空间.

8. 设  $\alpha, \beta$  是域  $F$  的某一个扩域内的元素,  $[F(\alpha) : F] = m$ ,  $[F(\beta) : F] = n$ , 证明,  $[F(\alpha, \beta) : F(\beta)] = m \iff [F(\alpha, \beta) : F(\alpha)] = n$ .

9. 设  $X^n - a$  是域  $F$  上一个多项式,  $\alpha$  是  $X^n - a$  在  $F$  的某个扩域  $K$  内的一个根,  $[F(\alpha) : F] = n$ . 令  $m$  是  $n$  的一个约数. 证明  $[F(\alpha^m) : F] = n/m$ ,  $[F(\alpha) : F(\alpha^m)] = m$ .

10. 设  $\alpha$  是域  $F$  上一个代数元,  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式, 设  $a \in F$ . 证明  $\alpha + a$  在  $F$  上的最小多项式是  $f(X - a)$ .

11. 设  $K$  是域  $F$  的一个扩域,  $u, v \in K$ , 其中  $v$  关于  $F$  是超越的, 而关于  $F(u)$  是代数的. 证明,  $u$  关于  $F(v)$  是代数的.

12. 令  $F = \mathbb{Z}/(2)$  是二元域. 找出  $F$  上一个二次不可约多项式  $f(X)$ , 并且添加  $f(X)$  的一个根  $\alpha$  于  $F$ , 得到一个四元域  $F(\alpha)$ .

用同样的方法构造一个  $F$  上的八元扩域  $K$ . 写出这八个元素, 并且证明它们正好是  $X^8 - X$  在  $K$  内的全部根.

13. 令  $F(X)$  是域  $F$  上不定元  $X$  的有理分式域,  $u =$

$X^3/X+1$ . 证明  $F(X)$  是  $F(u)$  上的单扩域, 并且求出  $[F(X):F(u)]$ .

14. 设  $\alpha$  是域  $F$  上一个代数元, 证明, 对于  $f(X) \in F[X]$  来说, 下列三个条件是等价的:

(i)  $f(X)$  是  $\alpha$  在  $F$  上最小多项式;

(ii)  $f(X)$  是一个最高次项系数为 1 的多项式, 并且满足条件: 对于任意  $g(X) \in F[X]$  来说,  $g(\alpha) = 0 \iff f(X) | g(X)$ .

(iii)  $f(X)$  是一个最高次项系数为 1 的多项式,  $f(\alpha) = 0$ , 并且对于任意  $0 \neq g(X) \in F[X]$  来说, 若  $g(\alpha) = 0$ , 则

$$\deg f < \deg g.$$

15. 设  $f(X) = X^4 + aX^2 + b^2$  是有理数域  $\mathbb{Q}$  上一个不可约多项式,  $\theta$  是  $f(X)$  在复数域内一个根. 证明,  $K = \mathbb{Q}(\theta)$  恰含有三个在  $\mathbb{Q}$  上是二次的子域.

16. 设  $F$  是一个特征不等于 2 的域,  $\alpha, \beta$  分别是  $F$  上不可约多项式  $X^2 - a$  和  $X^2 - b$  在  $F$  的某一个扩域内的根, 证明,  $F(\alpha) = F(\beta) \iff a = bc^2, c \in F$ .

17. 设  $\alpha \in \mathbb{C}$  是有理数域  $\mathbb{Q}$  上多项式  $X^3 - X^2 + X + 2$  的一个根. 将  $(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha)$  和  $(\alpha - 1)^{-1}$  表成  $a\alpha^2 + b\alpha + c$  ( $a, b, c \in \mathbb{Q}$ ) 的形式.

18. (Eisenstein 判断法), 设  $R$  是一个唯一分解整环,  $R[X]$  是  $R$  上不定元  $X$  的多项式环. 设

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in R[X].$$

如果存在  $R$  中一个素元  $p$ , 使得: (i)  $p \nmid a_0$ ; (ii)  $p | a_i, 1 \leq i \leq n$ ; (iii)  $p^2 \nmid a_n$ , 则  $f(X)$  不能分解成为  $R[X]$  中两个次数都低于  $n$  的多项式的乘积.

[注: 这个事实在以后的讨论中有时被用到, 证明时并不用域的知识.]

## 第二章 代数扩张

我们已经看到, 域  $F$  的一个扩域  $K$  的元素可以分成两类, 一类是  $F$  上的代数元, 另一类是  $F$  上的超越元. 如果  $K$  中每一个元素都是  $F$  上的代数元, 那么  $K$  就叫做  $F$  的一个代数扩域. 代数扩域是一种非常重要的扩域. 在这一章里, 我们将讨论这种扩域的一些基本性质.

### 2.1 代数扩域

设  $K$  是域  $F$  的一个扩域. 如果  $K$  的每一元素都是  $F$  上的代数元, 就称  $K$  是  $F$  的一个代数扩域, 这时  $K/F$  称为一个代数扩张; 在相反的情形, 也就是说, 如果  $K$  中存在  $F$  上的超越元, 就称  $K$  是  $F$  的一个超越扩域, 而  $K/F$  称为一个超越扩张.

**引理 2.1.1** 设  $K = F(\alpha_1, \dots, \alpha_n)$  是域  $F$  的一个有限生成的扩域, 而  $\alpha_1, \dots, \alpha_n$  都是  $F$  上代数元. 那么  $K$  是  $F$  上有限次扩域, 并且

$$K = F[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f(X_1, \dots, X_n) \in F[X_1, \dots, X_n]\},$$

$X_1, \dots, X_n$  是  $F$  上不相关不定元.

**证** 对生成元的个数  $n$  作归纳法.  $n = 1$  时,  $K = F(\alpha_1)$ ,  $\alpha_1$  是  $F$  上代数元. 由 1.3.2(i),  $K$  是  $F$  的有限次扩域, 并且  $K = F[\alpha_1]$ .

设  $n > 1$ , 并且假设对于  $n - 1$  来说, 定理成立, 现在设  $K = F(\alpha_1, \dots, \alpha_n)$ ,  $\alpha_1, \dots, \alpha_n$  是  $F$  上代数元. 令  $K' = F(\alpha_1, \dots, \alpha_{n-1})$ . 则  $K = K'(\alpha_n)$ ,  $F \subseteq K' \subseteq K$ . 由归纳法假设,  $[K' : F] < \infty$  且  $K' = F[\alpha_1, \dots, \alpha_{n-1}]$ ; 又  $[K : K'] < \infty$ , 所以

$$[K : F] = [K : K'] [K' : F] < \infty,$$

并且

$$K = K'[\alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = F[\alpha_1, \dots, \alpha_n]. \blacksquare$$

**定理 2.1.2** 设  $K$  是域  $F$  的一个扩域. 对于  $K$  来说, 以下两个条件是等价的:

- (i)  $K$  是  $F$  上有限次扩域;
- (ii)  $K$  是  $F$  上有限生成的代数扩域.

**证** (i)  $\implies$  (ii). 设  $[K : F] < \infty$ . 令  $\alpha$  是  $K$  中任意元素. 则  $F(\alpha) \subseteq K$ , 从而

$$[F(\alpha) : F] \leq [K : F] < \infty,$$

所以由 1.3.3,  $\alpha$  是  $F$  上代数元. 因此  $K/F$  是代数扩张. 令  $\alpha_1, \dots, \alpha_n \in K$  是  $K$  在  $F$  上的一个基. 则  $K = F(\alpha_1, \dots, \alpha_n)$ .

(ii)  $\implies$  (i) 由 2.1.1.  $\blacksquare$

**定理 2.1.3** 设  $L$  是域  $F$  的一个扩域,  $S$  是  $L$  的一个子集, 并且  $S$  的每一个元素都是  $F$  上代数元. 那么  $K = F(S)$  是  $F$  的一个代数扩域;  $K$  中每一元素  $\xi$  可以表成以下形式的有限项的和:

$$\xi = \sum a_{k_1 \dots k_m} \alpha_1^{k_1} \dots \alpha_m^{k_m},$$

这里  $\alpha_1, \dots, \alpha_m \in S$  (依赖于  $\xi$ ),  $a_{k_1 \dots k_m} \in F$ ,  $k_i$  是非负整数,  $i = 1, \dots, m$ .

**证** 令  $\{S_\alpha\}$  是  $S$  的有限子集族. 由 1.1.1 (ii),  $K = F(S) = \bigcup_\alpha F(S_\alpha)$ , 设  $\xi \in K$ . 那么存在  $S$  的一个有限子集  $S_\alpha = \{\alpha_1, \dots, \alpha_m\}$ . 使得

$$\xi \in F(S_\alpha) = F(\alpha_1, \dots, \alpha_m).$$

由 2.1.1 和 2.1.2,  $F(\alpha_1, \dots, \alpha_m)$  是  $F$  的代数扩域, 所以  $\xi$  关于  $F$  是代数的. 由于  $\xi$  是  $K$  任意元素, 所以  $K$  是  $F$  的代数扩域, 再由 2.1.1.  $\xi = f(\alpha_1, \dots, \alpha_m) \in F[\alpha_1, \dots, \alpha_m]$ .  $\blacksquare$

**推论 2.1.4** 设  $K$  是域  $F$  的一个扩域,  $\alpha, \beta \in K$  是  $F$  上代数元, 那么  $\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha\beta^{-1}$  (当  $\beta \neq 0$  时) 都是  $F$  上代数元.

**证** 在 2.1.3 中, 取  $S = \{\alpha, \beta\}$ , 则  $F(\alpha, \beta)$  是  $F$  的代数扩域. ■

**定理 2.1.5** 设  $K$  是域扩张  $L/F$  的一个中间域, 即  $F \subseteq K \subseteq L$ .  $L/F$  是代数扩张必要且只要  $L/K$  和  $K/F$  都是代数扩张.

**证** 必要性是显然的. 反之, 设  $L/K$  和  $K/F$  都是代数扩张. 设  $\xi \in L$ . 因为  $\xi$  关于  $K$  是代数的, 所以存在  $K[X]$  中非零多项式

$$g(X) = \sum_{j=0}^n \alpha_j X^j, \alpha_j \in K (0 \leq j \leq n),$$

使得  $g(\xi) = 0$ . 又  $K$  关于  $F$  是代数的, 所以  $\alpha_j (0 \leq j \leq n)$  是  $F$  上代数元. 于是由 2.1.1,  $K' = F(\alpha_0, \alpha_1, \dots, \alpha_n)$  是  $F$  的有限次扩域, 并且  $g(X) \in K'[X]$ . 因此  $\xi$  关于  $K'$  是代数的, 从而  $[K'(\xi) : K'] < \infty$ . 这样,

$$[K'(\xi) : F] = [K'(\xi) : K'] [K' : F] < \infty.$$

再由 2.1.1,  $K'(\xi)$  是  $F$  的代数扩域, 因而  $\xi$  是  $F$  上代数元. ■

**推论 2.1.6** 设

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K$$

是一个扩域序列, 这里  $F_i$  是  $F_{i-1}$  的扩域 ( $1 \leq i \leq n$ ). 那么  $K/F$  是代数扩张必要且只要每一  $F_i/F_{i-1}$  都是代数扩张 ( $1 \leq i \leq n$ ). ■

设  $K$  和  $E$  都是一个域  $L$  的子域.  $L$  中包含  $K$  和  $E$  的最小子域叫做  $K$  与  $E$  的合成域, 记作  $KE$ . 显然

$$KE = K(E) = E(K).$$

**定理 2.1.7** 设  $L$  是  $F$  域的一个扩域,  $K$  和  $E$  都是  $L/F$  的中间域.

(i) 如果  $K$  是  $F$  的代数扩域, 则  $KE$  是  $E$  的代数扩域.

(ii) 如果  $K$  和  $E$  都是  $F$  的代数扩域, 则  $KE$  也是  $F$  的代数

扩域.

证 (i)  $KE = E(K)$ , 而  $K$  的每一元素都是  $F$  上代数元, 所以也都是  $E$  上代数元, 由 2.1.3  $KE$  是  $E$  的代数扩域.

(ii) 由(i),  $KE$  是  $E$  的代数扩域, 而  $E$  又是  $F$  的代数扩域. 由 2.1.5,  $KE$  是  $F$  的代数扩域. ■

设  $K$  是域  $F$  的一个扩域. 令  $A$  是  $K$  中在  $F$  上的代数元的全体. 由 2.1.4,  $A$  是  $K$  的一个子域, 且  $F \subseteq A \subseteq K$ . 子域  $A$  叫做  $F$  在  $K$  中的代数闭包. 特别当  $F = A$  的, 就说  $F$  在  $K$  中是代数闭的.

例如, 有理数域  $Q$  在复数域  $C$  中的代数闭包就是代数数的全体.

**定理 2.1.8** 设  $K$  是域  $F$  的一个扩域,  $A$  是  $F$  在  $K$  中的代数闭包. 则  $A$  在  $K$  中是代数闭的.

证 令  $A'$  是  $A$  在  $K$  中的代数闭包. 我们有以下的一串扩域

$$F \subseteq A \subseteq A' \subseteq K.$$

$A/F$ ,  $A'/A$  都是代数扩张, 由 2.1.5,  $A'/F$  是代数扩张. 但  $A$  是  $F$  在  $K$  中的代数闭包, 所以  $A' \subseteq A$ , 从而  $A' = A$ . ■

**定理 2.1.9** 设  $X_1, \dots, X_n$  是域  $F$  上不相干不定元,  $K = F(X_1, \dots, X_n)$  是  $F$  上  $X_1, \dots, X_n$  的有理分式域. 那么  $F$  在  $K$  中是代数闭的.

证 对  $n$  作数学归纳法.

$n = 1$  时,  $K = F(X)$ ,  $X$  是  $F$  上不定元. 设  $\alpha \in K$ , 则

$$\alpha = f(X)/g(X), f(X), g(X) \in F[X], g(X) \neq 0.$$

设  $\alpha$  关于  $F$  是代数的. 如果  $\alpha \in F$ . 考虑域  $F(\alpha)$  上不定元  $T$  的多项式  $f(T) - \alpha g(T)$ . 则

$$f(T) - \alpha g(T) \neq 0.$$

事实上, 如果  $f(T) - \alpha g(T) = 0$ , 那么在  $f(T) - \alpha g(T)$  中,  $T$  的系数都是零. 然而这些系数都是  $\alpha$  的一次多项式, 系数属于  $F$ ,



由此就得出  $\alpha \in F$  的结论. 这就导致矛盾. 这样一来,  $X$  是  $F(\alpha)$  上非零多项式  $f(T) - \alpha g(T)$  的根, 从而  $X$  关于  $F(\alpha)$  是代数的. 又  $F(\alpha)$  是  $F$  的代数扩域, 所以  $X$  是  $F$  上代数元. 这又导致矛盾. 因此必须  $\alpha \in F$ ,  $F$  在  $K$  中代数闭.

现在设  $n > 1$  并且假设对于  $n - 1$  来说, 定理成立. 令  $F' = F(X, \dots, X_{n-1})$ , 则  $K = F'(X_n)$ , 设  $\alpha \in K$  关于  $F$  是代数的. 那么  $\alpha$  关于  $F'$  也是代数的, 由上面所证的  $n = 1$  的情形,  $F'$  在  $K$  中代数闭, 所以  $\alpha \in F'$ . 再由归纳法的假设,  $\alpha \in F$ . 所以  $F$  在  $K$  中是代数闭的. ■

## 习 题

1. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域. 令  $R = \{\sum_i x_i y_i \mid x_i \in K, y_i \in L\}$  (有限和). 证明:

- (i)  $R$  是  $M$  中包含  $K$  及  $L$  的一个子整环;
- (ii) 合成域  $KL$  是  $R$  的商域;
- (iii) 如果  $K$  或  $L$  是  $F$  的代数扩张, 则  $R = KL$ .

2. 设  $K$  是域  $F$  的一个扩域. 证明,  $K$  是  $F$  的代数扩域必要且只要任意满足条件  $F \subseteq A \subseteq K$  的子整环  $A$  都是子域.

3. 设  $F_1, F_2$  都是域  $K$  的子域,  $S$  是  $K$  的一个子集. 证明, 如果  $F_1$  的每一个元素都是  $F_2$  上的代数元, 则  $F_1(S)$  的每一个元素都是  $F_2(S)$  上的代数元.

4. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域. 证明:

- (i)  $[KL : F]$  是有限的必要且只要  $[K : F]$  和  $[L : F]$  都是有限的;
- (ii) 如果  $[KL : F]$  是有限的, 则  $[K : F]$  与  $[L : F]$  都整除  $[KL : F]$ , 且  $[KL : F] \leq [K : F][L : F]$ ;
- (iii) 如果  $[K : F]$  与  $[L : F]$  都是有限的且互素, 则  $[KL : L] = [K : F]$ .

5. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域且  $K$  和  $L$  都是  $F$  的有限次扩域.

(i) 证明, 如果  $[KL:F] = [K:F][L:F]$ , 则  $K \cap L = F$ .

(ii) 证明, 如果  $[K:F]$  或  $[L:F]$  等于 2, 那么 (i) 的逆命题也成立.

(iii) 举一反例说明, (i) 的逆命题一般不成立.

6. 设  $K$  是域  $F$  的一个有限次扩域. 证明, 如果对于  $K/F$  的任意两个中间域  $E_1, E_2$  来说, 要么  $E_1 \subseteq E_2$ , 要么  $E_2 \subseteq E_1$ , 则  $K$  是  $F$  的一个单扩域.

7. 设  $F$  是一个域且  $\text{char } F \neq 2$ .  $\alpha, \beta$  分别是  $F[X]$  中不可约多项式  $X^2 - a$  和  $X^2 - b$  在  $F$  的某一个扩域内的根. 证明,  $F(\alpha, \beta) = F(\alpha(\beta + 1))$ .

8. 设  $F$  是一个域且  $\text{char } F \neq 2$ ,  $K$  是  $F$  的一个四次扩域. 证明, 以下两个条件是等价的:

(i) 存在  $K/F$  的一个中间域  $E$ , 使得  $[E:F] = 2$ ;

(ii)  $K = F(\theta)$ ,  $\theta$  是  $F[X]$  中一个形如  $X^4 + aX^2 + b$  的不可约多项式的根.

9. 设  $\alpha$  是域  $F$  上不可约多项式  $X^2 - X - a$  的一个根. 证明, 对于  $K = F(\alpha)$  的元素  $\beta$  来说, 以下两个条件是等价的:

(i)  $\beta$  是  $F[X]$  中一个形如  $X^2 - X - b$  的不可约多项式的根;

(ii)  $\beta = c + (1 - 2c)\alpha$ , 其中  $c \in F$ ,  $2c \neq 1$ .

10. 设  $K$  是  $F$  域的一个代数扩域,  $N^+ = \{1, 2, 3, \dots\}$  是一切自然数所成的集. 证明:

(i) 存在  $K$  到  $F[X] \times N^+ = \{(f, i) | f \in F[X], i \in N^+\}$  内的一个单射;

(ii) 如果  $F$  是有限域, 则  $K$  的基数是至多可数的;

(iii) 如果  $F$  是无限域, 则  $K$  与  $F$  有相同的基数.

## 2.2 代数闭包

在这一节里, 我们要引进一个域的代数闭包的概念, 并且证明, 在同构的意义下, 每一个域恰有一个代数闭包.

**引理 2.2.1** 设  $F$  是一个域.  $f_i(X) \in F[X]$ ,  $1 \leq i \leq n$ , 是  $F$  上任意  $n$  个非常数多项式. 那么存在  $F$  的一个扩域  $K$  使得每一个  $f_i(X)$  在  $K$  中有一个根.

**证** 当  $n = 1$  时, 令  $p(X)$  是  $f_1(X)$  的一个不可约因式. 由 1.3.4, 存在  $F$  的扩域  $K$ , 使  $p(X)$  在  $K$  内有一个根  $\alpha$ , 从而  $f_1(\alpha) = 0$ .

设  $n > 1$ , 并且设对于  $n - 1$  来说引理成立, 于是存在  $F$  一个扩域  $K'$ , 使得  $f_1(X), \dots, f_{n-1}(X)$  在  $K'$  内各有一个根. 然而  $f_n(X) \in F[X] \subseteq K'[X]$ , 所以存在  $K'$  的一个扩域  $K$ , 使得  $f_n(X)$  在  $K$  内有一个根, 从而  $f_1(X), \dots, f_n(X)$  在  $K$  内各有一个根. ■

现在引入一个域的代数闭包的概念. 先引入代数闭域的概念.

一个域  $K$  说是代数闭的, 如果  $K[X]$  中每一次数大于零的多项式在  $K$  中有一个根.

**定义** 域  $F$  的一个扩域  $\Omega$  叫做  $F$  的一个代数闭包, 如果

(i)  $\Omega$  是  $F$  的代数扩域;

(ii)  $\Omega$  是代数闭域.

**定理 2.2.2** 设  $K$  是域  $F$  的一个扩域,  $A$  是  $F$  在  $K$  内的代数闭包. 如果  $K$  是代数闭域, 则  $A$  是  $F$  的一个代数闭包.

**证** 因为  $A$  是  $K$  中在  $F$  上的代数元的全体, 所以  $A$  是  $F$  的代数扩域. 我们证明,  $A$  是代数闭的. 设  $g(X) \in A[X]$  是一个次数大于零的多项式. 因为  $K$  是代数闭域, 所以  $g(X)$  在  $K$  内有一个根  $\alpha$ .  $\alpha$  关于  $A$  是代数的, 而由定理 2.1.8,  $A$  在  $K$  中是代数

闭的, 所以  $\alpha \in A$ . 这就证明了  $A$  是代数闭域. ■

**定理 2.2.3** 任意域  $F$  都有一个代数闭包.

**证** 证明分两步. 先证存在  $F$  的一个代数扩域, 使得  $F[X]$  每一个次数大于零的多项式在这个扩域里有一个根. 然后从  $F$  出发, 作一个串扩域

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$$

使得  $F_{i+1}$  是  $F_i$  的代数扩域, 并且  $F_i[X]$  中每一个次数大于零的多项式在  $F_{i+1}$  内有一个根 ( $i = 0, 1, 2, \dots$ ). 令  $\Omega = \bigcup_{i=0}^{\infty} F_i$ . 证明  $\Omega$

就是  $F$  的一个代数闭包.

先证第一步. 证明的思想与证明一个多项式的根的存在 (定理 1.3.4) 类似. 考虑  $F[X]$  中一切次数大于零的多项式的集

$$F[X] \setminus F = \{f_\lambda(X) \mid \lambda \in \Lambda\},$$

这里  $\Lambda$  是与  $F[X] \setminus F$  有相同基数的一个指标集. 对于每一个  $\lambda \in \Lambda$ , 令一个符号  $X_\lambda$  与它对应, 将  $\{X_\lambda\}_{\lambda \in \Lambda}$  看成  $F$  上不相关不定元, 即  $\{X_\lambda\}_{\lambda \in \Lambda}$  的任意有限子集都是  $F$  上不相关不定元. 令  $R = F[\{X_\lambda\}_{\lambda \in \Lambda}]$  表示  $\{X_\lambda\}_{\lambda \in \Lambda}$  的一切有限子集在  $F$  上所生成的多项式环的并集.  $R$  里每一个元素都是有限个不定元  $X_{\lambda_1}, \dots, X_{\lambda_r} \in \{X_\lambda\}_{\lambda \in \Lambda}$  在  $F$  上的多项式. 这样定义的  $R$  的元素是无歧义的. 显然, 一切  $f_\lambda(X_\lambda) \in R$  ( $\lambda \in \Lambda$ ).

令  $\alpha$  是由一切  $f_\lambda(X_\lambda)$ ,  $\lambda \in \Lambda$ , 所生的  $R$  的理想. 因为  $R$  是有单位元的交换环, 所以  $\alpha$  的元素都有以下形状:

$$(1) \quad \sum_k u_k f_k(X_k) \quad (\text{有限和}),$$

这里  $u_k$  是有限个  $X_\lambda$  ( $\lambda \in \Lambda$ ) 的多项式.  $\alpha$  是  $R$  的一个真子集, 因为不然的话, 将有  $1 \in \alpha$ , 从而可以表成 (1) 的形式:

$$1 = \sum_k u_k f_k(X_k).$$

右端只有有限个  $f_k(X_k)$  出现, 所以由 2.2.1, 存在  $F$  的一个扩

域, 使每一个  $f_k(X_k)$  在这个扩域中有一个根  $\alpha_k$ , 代入上式得出矛盾的等式  $1 = 0$ .

这样, 存在  $R$  的一个极大理想  $\mathfrak{m} \supseteq \mathfrak{a}$ . 令  $F_1 = R/\mathfrak{m}$ , 则  $F_1$  是一个域. 令

$$\varphi: R \rightarrow F_1 = R/\mathfrak{m}$$

是自然同态. 因为  $F \cap \mathfrak{m} = \{0\}$ , 所以  $\varphi|_F$  是单射, 因而可以把  $\varphi(F)$  与  $F$  等同起来, 而  $F$  可以认为是  $F_1$  的一个子域.

$F_1$  是  $F$  的代数扩域. 事实上, 设  $x_\lambda = \varphi(X_\lambda)$ , 则  $F_1$  是由  $\{x_\lambda\}_{\lambda \in \Lambda}$  在  $F$  上生成的域. 另一方面, 对于每一个  $\lambda \in \Lambda$ ,  $f_\lambda(X_\lambda) \in \mathfrak{a} \subseteq \mathfrak{m}$ . 所以  $f_\lambda(x_\lambda) = \varphi(f_\lambda(X_\lambda)) = 0$ . 因此  $x_\lambda$  是  $F$  上代数元. 由 2.1.3,  $F_1$  是  $F$  的代数扩域.

由于  $F_1$  是由一切  $f_\lambda(X_\lambda)$  的根  $x_\lambda$  在  $F$  上生成的, 这就证明了, 存在  $F$  的代数扩域  $F_1$ , 使得  $F[X]$  的每一个次数  $> 0$  的多项式  $f(X)$  在  $F_1$  中有一个根.

这样, 我们可以归纳地构造出一个扩域序列

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_i \subseteq F_{i+1} \subseteq \cdots,$$

使得

1°  $F_{i+1}$  是  $F_i$  的代数扩域;

2°  $F_i[X]$  的每一个次数  $> 0$  的多项式在  $F_{i+1}$  内有一个根,  $i = 0, 1, 2, \cdots$ .

令  $\Omega = \bigcup_{i=0}^{\infty} F_i$ , 容易证明,  $\Omega$  是一个域. 我们证明,  $\Omega$  是  $F$

的一个代数闭包.

首先,  $\Omega$  是  $F$  代数扩域. 设  $\alpha \in \Omega$ , 那么存在  $i$ , 使得  $\alpha \in F_i$ ,  $F_i$  是  $F$  的代数扩域, 所以  $\alpha$  是  $F$  上的代数元.

其次,  $\Omega$  是代数闭的. 设

$$f(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n \in \Omega[X],$$

$n > 0$ ,  $\alpha_i \in \Omega$ ,  $i = 0, 1, \cdots, n$ . 于是存在一个整数  $k > 0$ ,

使得  $\alpha_i \in F_k$ ,  $i = 0, 1, \dots, n$ .  $f(X) \in F_k[X]$ , 所以  $f(X)$  在  $F_{k+1}$  内有一个根, 因而在  $\Omega$  内有一个根.

这就证明了  $\Omega$  是  $F$  的代数闭包. ■

**定理 2.2.4** 设  $\varphi: F \rightarrow F'$  是域  $F$  到域  $F'$  的一个同构映射,  $\Omega$  和  $\Omega'$  各是  $F$  和  $F'$  的一个代数闭包. 那么  $\varphi$  可以开拓为  $\Omega$  到  $\Omega'$  的同构, 即存在域同构  $\psi: \Omega \rightarrow \Omega'$ , 使得  $\psi|_F = \varphi$ .

特别, 一个域  $F$  的任意两个代数闭包都是同构的.

**证** 显然, 取  $F' = F$ ,  $\varphi$  是  $F$  的恒等的同构, 则最后论断可以由前一个论断直接得出. 因此只要证明前一论断. 设  $K$  是域扩张的一个中间域. 令  $\psi$  是  $\varphi$  到  $K$  上的一个开拓, 即  $\psi: K \rightarrow \Omega'$  是一个单同态并且  $\psi|_F = \varphi$ . 考虑一切这样的对  $(K, \psi)$  所成的集  $S$ .  $S$  不空, 因为  $(F, \varphi) \in S$ . 对于  $S$  中任意两个元素  $(K_1, \psi_1)$ ,  $(K_2, \psi_2)$ , 规定,

$$(K_1, \psi_1) \leq (K_2, \psi_2), \text{ 如果 } K_1 \subseteq K_2 \text{ 且 } \psi_2|_{K_1} = \psi_1.$$

这样一来,  $S$  作成是一个偏序集. 我们证明,  $S$  是一个归纳集. 设

$$S' = \{(K_\lambda, \psi_\lambda) \mid \lambda \in \Lambda\}$$

是  $S$  的一个非空链, 令

$$K = \bigcup_{\lambda \in \Lambda} K_\lambda.$$

$K$  显然是  $\Omega$  的一个子域. 设  $\alpha \in K$ , 那么  $\alpha$  属于某一  $K_\lambda$ ,  $\lambda \in \Lambda$ , 因此, 对于任意  $\mu \in \Lambda$ , 如果  $K_\lambda \subseteq K_\mu$ , 则  $\alpha \in K_\mu$ , 我们如下地定义  $\psi: K \rightarrow \Omega'$ . 如果  $\alpha \in K_\lambda$ , 则定义  $\psi(\alpha) = \psi_\lambda(\alpha)$ . 因为当  $K_\lambda \subseteq K_\mu$  时,  $\psi_\mu|_{K_\lambda} = \psi_\lambda$ , 所以这样定义是无歧义的, 并且  $\psi$  是  $K$  到  $\Omega'$  内的单同态. 这样,  $(K, \psi) \in S$ .  $(K, \psi)$  是  $S'$  的一个上界. 于是由 Zorn 引理,  $S$  有一个极大元素  $(L, \omega)$ . 因为  $\Omega$  是  $F$  的代数扩域, 所以  $\Omega$  也是  $L$  的代数扩域.

我们证明,  $L = \Omega$ . 且  $\omega(L) = \omega(\Omega) = \Omega'$ .

设  $\alpha \in \Omega$ , 令  $p(X) \in L[X]$  是  $\alpha$  在  $L$  上的最小多项式. 令  $L' = \omega(L) \subseteq \Omega'$ .  $\omega$  可以通过自然的方式开拓为环同构  $L[X] \rightarrow L'[X]$ , 我们仍用  $\omega$  表示这个环同构. 对于  $f(X) \in L[X]$ ,  $\omega(f(X))$  就是把  $f(X)$  的系数  $a_i$  相应地换成  $\omega(a_i)$  所得的  $L'$  上的多项式. 因为  $p(X)$  是  $L[X]$  中不可约多项式, 容易证明  $p'(X) = \omega(p(X))$  是  $L'[X]$  中不可约多项式. 因此, 剩余类环  $L[X]/(p(X))$  和  $L'[X]/(p'(X))$  都是域, 并且  $\omega$  诱导出域同构  $\bar{\omega} : L[X]/(p(X)) \rightarrow L'[X]/(p'(X))$ .

因为  $\Omega'$  是代数闭域, 所以存在  $\alpha' \in \Omega'$ , 使得  $p'(\alpha') = 0$ . 因为  $p'(X)$  是  $L'[X]$  中最高次项系数是 1 的不可约多项式, 所以  $p'(X)$  就是  $\alpha'$  在  $L'$  上的最小多项式. 于是由 1.3.1, 分别存在域同构

$\sigma : L(\alpha) \rightarrow L[X]/(p(X))$  和  $\sigma' : L'(\alpha') \rightarrow L'[X]/(p'(X))$   
 $\sigma|_L = 1_L$ , 且  $\sigma'|_{L'} = 1_{L'}$ . 令

$$\tau = \sigma'^{-1} \circ \omega \circ \sigma,$$

则  $\tau : L(\alpha) \rightarrow L'(\alpha') \subseteq \Omega'$  是  $L(\alpha)$  到  $\Omega'$  内的单同态. 对于任意  $\xi \in L$ , 我们有  $\tau(\xi) = \omega(\xi)$ . 所以  $(L(\alpha), \tau) \in S$  并且  $(L, \omega) \leq (L(\alpha), \tau)$ . 由  $(L', \omega)$  的极大性得

$$L(\alpha) = L, \quad \tau = \omega$$

这样,  $\Omega$  的任意元都在  $L$  内, 所以  $L = \Omega$ .

设  $\Omega'' = \omega(L) = \omega(\Omega) \subseteq \Omega'$ . 则  $\Omega''$  是代数闭域而  $\Omega'$  是  $\Omega''$  的代数扩域, 所以  $\Omega'' = \Omega'$ , 即  $\omega(\Omega) = \Omega'$ . ■

**推论 2.2.5** 设  $\Omega$  是域  $F$  的一个代数闭包, 而  $K$  是  $F$  的一个代数扩域. 则  $L$  与  $\Omega/F$  的一个中间域同构.

**证** 令  $\Omega'$  是  $K$  的一个代数闭包. 则  $\Omega'$  也是  $F$  的一个代数闭包. 由 2.2.4, 存在域同构  $\sigma : \Omega' \rightarrow \Omega$ . 且  $\sigma|_F$  就是  $F$  的恒等自同构. 令  $E = \sigma(K)$ . 则  $E$  是  $\Omega/F$  的一个中间域. ■

以下为了叙述简便起见, 我们引进一个术语. 设  $K$  和  $L$  都是

域  $F$  的扩域. 同态或同构映射  $\varphi: K \rightarrow L$  叫做一个  $F$ -同态或  $F$ -同构, 如果  $\varphi|_F$  是  $F$  的恒等自同构.

**推论 2.2.6** 设  $\Omega$  是域  $F$  的一个代数闭包,  $K$  是  $\Omega/F$  的一个中间域,  $\varphi: K \rightarrow \Omega$  是一个  $F$ -单同态. 那么  $\varphi$  总可以开拓成为  $\Omega$  的一个  $F$ -自同构.

**证**  $\Omega$  是  $K$  和  $\varphi(K)$  的代数闭包. 由定理 2.2.4, 存在  $\Omega$  的一个  $F$ -自同构  $\omega$ , 使得  $\omega|_K = \varphi$ . ■

**推论 2.2.7** 设  $\Omega$  是域  $F$  的一个代数闭包. 对于  $\Omega$  的元素  $\alpha, \beta$  来说, 以下两个条件是等价的:

- (i)  $\beta$  是  $\alpha$  在  $F$  上最小多项式  $p(X)$  的根;
- (ii) 存在  $\Omega$  的一个  $F$ -自同构  $\omega$ , 使得  $\omega(\alpha) = \beta$ .

**证** (i)  $\implies$  (ii)  $p(X)$  也是  $\beta$  在  $F$  上的最小多项式. 因此, 存在  $F$ -同构

$$\varphi = F(\alpha) \cong F[X]/(p(X)) \cong F(\beta),$$

且  $\varphi(\alpha) = \beta$ . 由 2.2.6,  $\varphi$  可以开拓成为  $\Omega$  的一个同构  $\omega$ .

(ii)  $\implies$  (i) 设存在  $\Omega$  的一个  $F$ -自同构  $\omega$ , 使得  $\omega(\alpha) = \beta$ . 于是

$$p(\beta) = p(\omega(\alpha)) = \omega(p(\alpha)) = 0. \quad \blacksquare$$

## 习 题

1. 设  $F$  是一个域. 如果对于  $F$  的每一个扩域  $K$  来说,  $F$  的包含在  $K$  内的最大代数扩域就是  $F$  本身, 则  $F$  是代数闭的.

2. 设  $L$  是域  $F$  的一个代数扩域. 证明, 对于  $L$  来说, 下列三条件等价:

- (i)  $L$  是  $F$  的代数闭包;
- (ii) 对于  $F$  的任意一个代数扩域  $K$  来说, 存在一个  $F$ -同态单射  $\varphi: K \rightarrow L$ ;

(iii) 设  $\sigma: F' \rightarrow F$  是一个域同构. 那么对于  $F'$  的每一个



代数扩域 $K'$ 来说,  $\sigma$ 可以开拓为域同态单射 $K' \rightarrow L$ .

3. 设 $K$ 是域 $F$ 的一个代数扩域. 证明, 如果 $F[X]$ 中每一个次数大于零的多项式在 $K[X]$ 内可以分解成一次因式的乘积, 那么 $K[X]$ 的每一个次数大于零的多项式在 $K[X]$ 内也可以分解成一次因式的乘积.

4. 设 $F \subseteq K \subseteq L$ 是一串扩域, 其中 $F$ 在 $K$ 内是代数闭的. 又设 $\alpha \in L$ 是 $F$ 上一个代数元. 证明,  $[K(\alpha) : K] = [F(\alpha) : F]$ .

5. 设 $F \subseteq E \subseteq K \subseteq L$ 是一串扩域,  $F$ 在 $K$ 内是代数闭的且 $[K : E] < \infty$ . 又设 $\alpha \in L$ 是 $F$ 上一个代数元. 证明,  $[K(\alpha) : E(\alpha)] = [K : E]$ .

6. 设 $K = \mathbb{Q}(\alpha) \subseteq \mathbb{C}$ 是 $\mathbb{Q}$ 上一个单代数扩域且 $\alpha \neq \bar{\alpha}$ ,  $\bar{\alpha} \in K$  (这里 $\bar{\alpha}$ 表示 $\alpha$ 的共轭复数). 证明:

(i)  $[K : \mathbb{Q}]$ 是一个偶数, 并且存在 $K$ 在 $\mathbb{Q}$ 上具有以下形状的一个基:

$$\gamma_1, \bar{\gamma}_1, \gamma_2, \bar{\gamma}_2, \dots, \gamma_m, \bar{\gamma}_m.$$

(ii) 令 $K_0 = K \cap \mathbb{R}$ . 则 $\gamma_1 + \bar{\gamma}_1, \dots, \gamma_m + \bar{\gamma}_m$ 是 $K_0$ 在 $\mathbb{Q}$ 上的一个基.

### 2.3 正规扩域 多项式的分裂域

在这一节里, 我们将介绍一个域 $F$ 上的一种很重要的代数扩域, 称为正规扩域. 正规扩域和 $F$ 上一个多项式的分裂域有着密切的关系. 我们将把这两个概念结合在一起讨论.

先指出一个简单的事实. 设 $F$ 和 $F'$ 都是域. 如果存在 $F$ 到 $F'$ 的一个同态映射 $\sigma : F \rightarrow F'$ , 那么 $\sigma$ 可以用自然的方式开拓成为多项式环 $F[X]$ 到 $F'[X]$ 的同态映射. 即对于

$$f(X) = a_0 + a_1 X + \dots + a_n X^n \in F[X],$$

定义

$$\sigma(f(X)) = \sigma(a_0) + \sigma(a_1)X + \dots + \sigma(a_n)X^n \in F'[X]$$

以后我们对记号  $\sigma(f(X))$  都作这样的理解。特别，当  $\sigma$  是  $F$  到  $F'$  的同构映射时， $\sigma : F[X] \rightarrow F'[X]$  也是同构映射。

**引理 2.3.1** 设  $K$  是域  $F$  的一个代数扩域。那么  $K$  到  $K$  自身的每一个  $F$ -同态单射都是满的，因而是  $F$ -自同构。

**证** 设  $\sigma : K \rightarrow K$  是一个同态单射，且保持  $F$  的元素不动。设  $\alpha \in K$ 。则  $\alpha$  是  $F$  上代数元。令  $p(X)$  是  $\alpha$  在  $F$  上的最小多项式。设  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$  是  $p(X)$  在  $K$  内的一切互不相同的根。则在  $K[X]$  内我们有

$$p(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_m)^{k_m} g(X),$$

这里  $k_1, \dots, k_m \geq 1$ ， $g(X) \in K[X]$  且在  $K$  内没有根。对这个等式两端的系数作用  $\sigma$ ，因为  $p(X) \in F[X]$ ，所以  $\sigma(p(X)) = p(X)$ 。于是

$p(X) = \sigma(p(X)) = (X - \sigma(\alpha_1)^{k_1} \cdots (X - \sigma(\alpha_m)^{k_m} \sigma(g(X)))$   
 $\sigma(g(X)) \in K[X]$ 。因为  $\sigma$  是单射，所以  $\sigma(\alpha_1), \dots, \sigma(\alpha_m)$  仍是  $p(X)$  在  $K$  内一切互不相同的根。所以

$$\{\sigma(\alpha_1), \dots, \sigma(\alpha_m)\} = \{\alpha_1, \dots, \alpha_m\}.$$

这样一来， $\alpha$  等于某个  $\sigma(\alpha_i)$ ，即  $\alpha \in \sigma(K)$ 。所以  $\sigma$  是满射。 ■

现在引入一个概念。设  $E$  和  $E'$  都是域  $F$  的扩域。如果

- (i)  $E$  和  $E'$  都是  $F$  的某一扩域  $L$  的子域；
- (ii) 存在一个  $F$ -同构  $\varphi : E \rightarrow E'$ 。

那么就说， $E$  与  $E'$  在  $F$  上**共轭**，简称 **$F$ -共轭**。在不致引起混淆的情况下，就称  $E$  与  $E'$  **共轭**。如果  $E$  与  $E'$  共轭，那么就称  $E$  到  $E'$  的  $F$ -同构映射为  **$F$ -共轭映射**。

**定义** 设  $F$  是一个域。  $F$  上一个扩域  $E$  叫做一个**正规扩域**，如果下列条件被满足：

- (i)  $E$  是  $F$  的代数扩域<sup>1)</sup>；

---

1) 在正规扩域的定义中，条件(i)实际上是多余的，在第四章我们将证明，满足条件(ii)的扩域一定是代数的(参看4.1.1.3)。

(ii) 任意与  $E$  在  $F$  上共轭的域都等于  $E$ 。

如果  $E$  是  $F$  的一个正规扩域, 那么也说  $E/F$  是一个正规扩张。

例 1 令  $\mathbb{Q}$  是有理数域,  $E = \mathbb{Q}(\sqrt{2})$ . 则  $E$  是  $\mathbb{Q}$  的一个正规扩域. 事实上, 设  $\sigma$  是  $E$  的一个  $\mathbb{Q}$ -共轭. 则  $\sigma(\sqrt{2})$  是  $\sigma(X^2 - 2) = X^2 - 2$  的一个根. 然而  $X^2 - 2$  在  $E$  的任意一个扩域内只有两个根:  $\sqrt{2}$  和  $-\sqrt{2}$ , 所以  $\sigma(\sqrt{2}) = \sqrt{2}$  或  $-\sqrt{2}$ . 不论哪一个情形都有  $\sigma(E) = \mathbb{Q}(\sigma(\sqrt{2})) = \mathbb{Q}(\sqrt{2}) = E$ .

例 2  $E = \mathbb{Q}(\sqrt[3]{2})$  不是  $\mathbb{Q}$  的正规扩域. 因为在复数域  $\mathbb{C}$  内,  $X^3 - 2$  有三个根:  $\sqrt[3]{2}$ ,  $\xi\sqrt[3]{2}$ ,  $\xi^2\sqrt[3]{2}$ , 这里  $\xi = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$  是一个三次单位根. 显然  $E' = \mathbb{Q}(\xi\sqrt[3]{2})$  是一个与  $E$   $\mathbb{Q}$ -共轭的域, 但  $E' \neq E$ .

定理 2.3.2 设  $E$  是域  $F$  的一个代数扩域. 对于  $E/F$  来说, 下列三个条件是等价的:

(i)  $E/F$  是正规扩张;

(ii) 设  $\Omega$  是  $F$  的任意一个包含  $E$  的代数闭包. 那么对于  $\Omega$  的任意一个  $F$ -自同构  $\sigma$ , 都有  $\sigma(E) = E$ .

(iii)  $E$  的任意元素  $\alpha$  在  $F$  上的最小多项式在  $E[X]$  中可以分解为一次因式的乘积.

证 (i)  $\implies$  (ii) 设  $\Omega$  是  $F$  的一个代数闭包且包含  $E$ .  $\Omega$  的任意一个自同构  $\sigma$  将  $E$  映成一个与  $E$  是  $F$ -共轭的域  $\sigma(E)$ . 因为  $E$  是  $F$  的正规扩域, 所以  $\sigma(E) = E$ .

(ii)  $\implies$  (iii) 设  $\Omega$  是  $F$  的一个包含  $E$  的代数闭包.  $\alpha \in E$  在  $F$  上的最小多项式  $p(X)$  在  $\Omega[X]$  内分解成一次因式的积:

$$p(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n);$$

$\alpha_i \in \Omega$ ,  $1 \leq i \leq n$ , 且设  $\alpha_1 = \alpha$ . 由推论 2.2.7, 存在的  $\Omega$  的  $F$ -自同构  $\sigma_i$ , 使得  $\sigma_i(\alpha) = \alpha_i$ ,  $1 \leq i \leq n$ . 因为  $\alpha_i \in \sigma_i(E) =$

$E (1 \leq i \leq n)$ , 所以  $p(X)$  在  $E[X]$  中可以分解成一次因式的积.

(iii)  $\implies$  (i) 设  $E'$  是一个与  $E$  为  $F$ -共轭的域, 由共轭的定义,  $E$  和  $E'$  都包含在  $F$  的某一扩域  $L$  内, 并且存在  $F$ -同构映射  $\psi: E \rightarrow E'$ . 设  $\alpha' \in E'$ , 令  $\alpha = \psi^{-1}(\alpha') \in E$ . 令  $p(X)$  是  $\alpha$  在  $F$  上最小多项式. 由 (iii),  $p(X)$  在  $E[X]$  内可以分解成一次因式的积:

$$p(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n), \alpha_i \in E (1 \leq i \leq n).$$

因为  $p(\alpha) = 0$ , 所以  $p(\alpha') = \psi(p(\alpha)) = 0$ . 因此, 在  $L$  内, 等式

$$(\alpha' - \alpha_1)(\alpha' - \alpha_2) \cdots (\alpha' - \alpha_n) = 0$$

成立. 于是  $\alpha'$  必定等于某一个  $\alpha_i$ , 从而,  $\alpha' \in E$ . 因为  $\alpha'$  是  $E'$  的任意元素, 所以  $E' \subseteq E$ .

这样,  $\psi: E \rightarrow E' \subseteq E$  是  $E$  到自身内的一个同态单射. 因为  $E$  是  $F$  的代数扩域, 由 2.3.1,  $\psi$  是满射, 从而  $E' = \psi(E) = E$ . 这就证明了  $E$  的任意一个  $F$ -共轭的域都与  $E$  相等, 即  $E$  是  $F$  的正规扩域. ■

**推论 2.3.3** 设  $E$  是域  $F$  的一个正规扩域. 对于  $E$  的元素  $\alpha$  与  $\beta$  来说, 以下两个条件是等价的:

(i)  $\alpha$  与  $\beta$  在  $F$  上有同一个最小多项式;

(ii) 存在  $E$  的一个  $F$ -自同构  $\sigma$ , 使得  $\sigma(\alpha) = \beta$ .

**证** (i)  $\implies$  (ii) 设  $\Omega$  是  $E$  的一个代数闭包.  $\Omega$  显然是  $F$  的一个包含  $E$  的代数闭包. 由 2.2.7, 存在  $\Omega$  的一个  $F$ -自同构  $\tau$ , 使得  $\tau(\alpha) = \beta$ .  $E$  和  $\tau(E)$  都是  $\Omega/F$  的中间域, 且是  $F$ -共轭的. 由于  $E$  是正规的, 所以  $\tau(E) = E$ . 这样,  $\sigma = \tau|_E$  是  $E$  的一个  $F$ -自同构, 并且  $\sigma(\alpha) = \beta$ .

(ii)  $\implies$  (i) 设  $p(X)$  是  $\alpha$  在  $F$  上的最小多项式. 那么

$$p(\beta) = p(\sigma(\alpha)) = \sigma(p(\alpha)) = 0.$$

所以  $p(X)$  也是  $\beta$  在  $F$  上的最小多项式. ■

现在我们引入域  $F$  上一个多项式的分裂域的概念.

**定义** 设  $f(X)$  是域  $F$  上一个次数大于 0 的多项式.  $F$  的一个扩域  $K$  叫做  $f(X)$  在  $F$  上一个**分裂域**, 如果

(i)  $f(X)$  在  $K[X]$  中可以分解成为一次因式的乘积:

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n),$$

$$a \in F, \alpha_i \in K (1 \leq i \leq n);$$

(ii)  $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ .

$F[X]$  中任意一个次数大于 0 的多项式在  $F$  上总存在分裂域. 事实上, 取  $F$  上一个代数闭包  $\Omega$ . 则  $f(X)$  在  $\Omega[X]$  可以分解成为一次因式的积. 将  $f(X)$  在  $\Omega$  内的全部根添加到  $F$  上所得到的扩域  $K$  就是  $f(X)$  在  $F$  上的一个分裂域.

**定理 2.3.4** 设  $f(X)$  是域  $F$  上一个次数大于 0 的多项式,  $K$  和  $K'$  都是  $f(X)$  在  $F$  上的分裂域. 在  $K[X]$  和  $K'[X]$  里, 分别有

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n),$$

$$f(X) = a(X - \alpha'_1)(X - \alpha'_2) \cdots (X - \alpha'_n),$$

$\alpha_i \in K, \alpha'_i \in K' (1 \leq i \leq n), a \in F$ , 那么存在  $K$  到  $K'$  的一个  $F$ -同构映射  $\varphi$ . 使得

$$\{\varphi(\alpha_1), \dots, \varphi(\alpha_n)\} = \{\alpha'_1, \dots, \alpha'_n\}.$$

**证** 令  $\Omega$  和  $\Omega'$  分别是  $K$  和  $K'$  的代数闭包. 它们也是  $F$  的代数闭包. 由定理 2.2.4, 存在一个  $F$ -同构映射  $\omega: \Omega \rightarrow \Omega'$ . 令  $\alpha''_i = \omega(\alpha_i), 1 \leq i \leq n; K'' = F(\alpha''_1, \dots, \alpha''_n)$ . 在  $K''[X]$  内,

$$f(X) = a(X - \alpha''_1)(X - \alpha''_2) \cdots (X - \alpha''_n).$$

因为  $K'' \subseteq \Omega'$ , 所以在  $\Omega'[X]$  内,  $f(X)$  有两种分解:

$$\begin{aligned} f(X) &= a(X - \alpha'_1)(X - \alpha'_n) \cdots (X - \alpha'_n) \\ &= a(X - \alpha''_1)(X - \alpha''_2) \cdots (X - \alpha''_n). \end{aligned}$$

由域上多项式因式分解的唯一性, 我们有

$$\{\omega(\alpha_1), \dots, \omega(\alpha_n)\} = \{\alpha'_1, \dots, \alpha'_n\},$$

从而  $K'' = K'$ . 令  $\varphi = \omega|_K$  就满足要求. ■

下面的定理表明正规扩域和多项式的分裂域这两个概念的密切联系。

**定理 2.3.5** 设  $K$  是域  $F$  的一个扩域。对于  $K$  来说，以下两个条件是等价的；

(i)  $K$  是  $F$  的有限次正规扩域；

(ii)  $K$  是  $F[X]$  的某一次数大于零的多项式在  $F$  上的分裂域。

**证** (i)  $\implies$  (ii)  $K$  是  $F$  的有限次扩域，由定理 2.1.2,  $K = F(\alpha_1, \dots, \alpha_s)$ ,  $\alpha_i$  是  $F$  上代数元 ( $1 \leq i \leq s$ )。令  $p_i(X)$  是  $\alpha_i$  在  $F$  上的最小多项式。令

$$f(X) = \prod_{i=1}^s p_i(X).$$

由定理 2.3.2 (iii), 每一个  $p_i(X)$  在  $K[X]$  内可以分解成一次因式的乘积：

$$p_i(X) = \prod_{j=1}^{n_i} (X - \alpha_{ij}), \alpha_{ij} \in K, 1 \leq i \leq s.$$

于是在  $K[X]$  内，

$$f(X) = \prod_{i=1}^s \prod_{j=1}^{n_i} (X - \alpha_{ij}).$$

于是

$$K = F(\alpha_1, \dots, \alpha_s) \subseteq F(\{\alpha_{ij}\});$$

$$1 \leq i \leq s, 1 \leq j \leq n_i.$$

所以  $K$  是  $f(X)$  在  $F$  上的分裂域。

(ii)  $\implies$  (i) 设  $K$  是  $F[X]$  中某一次数大于 0 的多项式  $f(X)$  在  $F$  上的分裂域。取  $K$  的一个代数闭包  $\Omega$ , 它也是  $F$  的代数闭包。在  $\Omega[X]$  中，

$$f(X) = a(X - \alpha_1) \cdots (X - \alpha_n), a \in F, \alpha_i \in \Omega.$$

那么  $K = F(\alpha_1, \dots, \alpha_n)$ , 由定理 2.1.2,  $[K : F] < \infty$ .

设  $\sigma$  是  $\Omega$  的任意一个  $F$ -自同构.  $\sigma$  自然地开拓为多项式环  $\Omega[X]$  的自同构, 仍以  $\sigma$  表示. 因为  $\sigma$  保持  $F$  的元素不动, 我们有

$$f(X) = \sigma(f(X)) = a(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n)).$$

由  $\Omega[X]$  中多项式因式分解的唯一性, 我们有

$$\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\} = \{\alpha_1, \dots, \alpha_n\}.$$

所以  $K = F(\alpha_1, \dots, \alpha_n) = F(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = \sigma(K)$ . 由 2.3.2,  $K$  是  $F$  上的正规扩域. ■

由这个定理可以得出以下的推论. 我们把这个推论的证明留给读者.

**推论 2.3.6** 设  $K$  是域  $F$  上的一个有限次扩域. 对于  $K$  来说, 以下两个条件是等价的:

(i)  $K$  是  $F[X]$  中某一个次数大于零的多项式在  $F$  上的分裂域;

(ii)  $F[X]$  内任意一个不可约多项式如果在  $K$  内有一个根, 那么它在  $K[X]$  内可以分解成一次因式的乘积. ■

## 习 题

1. 证明,  $K/F$  是代数域扩张的充分且必要的条件是, 对于  $K/F$  的每一个中间域  $E$  来说, 如果  $\sigma: E \rightarrow E$  是  $F$ -同态单射, 则  $\sigma$  必是  $E$  的  $F$ -自同构.

2. 试举一反例说明, 当  $K$  不是域  $F$  的代数扩域时, 定理 2.3.1 的结论不成立.

3. 下列域扩张哪些是正规扩张:

$$(i) \quad \mathbb{Q}(\sqrt{-3})/\mathbb{Q}; \quad (ii) \quad \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q};$$

$$(iii) \quad \mathbb{C}/\mathbb{R}; \quad (iv) \quad \mathbb{C}/\mathbb{Q}.$$

4. 证明, 一个域  $F$  的二次扩域一定是  $F$  的正规扩域.

5. 设  $F \subseteq K \subseteq L$  是一串扩域, 其中  $L/F$  是正规扩张.  $L/K$  是否正规?  $K/F$  是否正规?

如果  $L/K$  及  $K/F$  都是正规扩张, 那么  $L/F$  是否正规?

6. 设  $F[X]$  是域  $F$  上一个不定元的多项式环,  $\{f_\lambda\}_{\lambda \in \Lambda}$ , 其中  $\Lambda$  是一个指标集(有限或无限),  $\Omega$  是  $F$  的一个代数闭包, 令  $K$  是将  $\{f_\lambda\}_{\lambda \in \Lambda}$  在  $\Omega$  内的一切零点添加到  $F$  所得的扩域, 证明,  $K$  是  $F$  的正规扩域.

7. 设  $K$  是域  $F$  的一个代数扩域,  $N$  是  $F$  的一个包含  $K$  的正规扩域. 证明,  $K/F$  是正规扩张必要且只要  $K$  到  $N$  内的每一个  $F$ -同态单射都是  $K$  的自同构.

8. 设  $K$  是域  $F$  的一个代数扩域. 证明, 如果  $K$  的每一个元素都属于某一个中间域  $E$ , 而  $E$  是  $F$  的正规扩域, 则  $K$  是  $F$  的正规扩域.

9. 设  $\Omega$  是域  $F$  的一个代数闭包,  $N_\lambda \subseteq \Omega$  ( $\lambda$  取遍某一个指标集  $\Lambda$ ) 都是  $F$  的正规扩域. 令  $N_1 = \bigcap_{\lambda \in \Lambda} N_\lambda$ ,  $N_2 = F(\bigcup_{\lambda \in \Lambda} N_\lambda)$ . 证明,  $N_1, N_2$  都是  $F$  的正规扩域.

10. 设  $f(X)$  是域  $F$  上一个  $n$  ( $n > 0$ ) 次多项式,  $K$  是  $f(X)$  在  $F$  上一个分裂域. 证明,  $[K:F] \mid n!$ .

11. 设  $K$  是域  $F$  的一个代数扩域. 证明, 对于  $K$  来说, 以下两个条件是等价的:

(i)  $K$  是  $F$  的正规扩域;

(ii)  $F[X]$  中每一个不可约多项式  $f(X)$  在  $K[X]$  中若分解成为不可约因式的乘积, 则所有这些不可约因式都有相同的次数.

12. 证明推论 2.3.6.



## 2.4 有限域

只含有有限个元素的域叫做有限域。有限域的构造特别简单。在这一节里，我们将对于有限域作一比较全面的讨论。

设  $F$  是一个有限域。那么  $F$  所包含的素域  $P$  也是一个有限域。由 1.2.1，这个素域所含的元素个数是一个素数  $p$ 。因此  $\text{char } F = p$ 。

设  $F$  含有  $q$  个元素， $F$  是素域  $P$  上有限次扩域。设  $[F : P] = f$ ，而  $\alpha_1, \dots, \alpha_f$  是  $F$  在  $P$  上一个基，那么  $F$  的每一个元素  $\alpha$  可以唯一地表示成

$$\alpha = a_1 \alpha_1 + \dots + a_f \alpha_f$$

的形式， $a_i \in P$ ， $1 \leq i \leq f$ 。因此  $q = p^f$ 。

令  $F^\times = F \setminus \{0\}$  是  $F$  的一切非零元素所组成的集。则  $F^\times$  是一个  $q - 1$  阶乘法群。 $F^\times$  的每一个元素都是方程  $X^{q-1} - 1 = 0$  的根。另一方面， $X^{q-1} - 1 = 0$  在  $F$  中至多有  $q - 1$  个根，所以

$$X^{q-1} - 1 = \prod_{\alpha \in F^\times} (X - \alpha).$$

这样， $F$  是多项式  $X^{q-1} - 1$  在素域  $P$  上的分裂域。同时  $F$  的每一个元素都是多项式

$$X^q - X = \prod_{\alpha \in F} (X - \alpha)$$

的根，所以  $F$  也是多项式  $X^q - X$  在  $P$  上的分裂域。

总结上面的讨论，我们得到

**定理 2.4.1** 设  $F$  是一个  $q$  元有限域， $P$  是  $F$  的素域。

(i)  $\text{char } F = p > 0$ ； $q = p^f$ ； $[F : P] = f$ 。

(ii)  $X^q - X = \prod_{\alpha \in F} (X - \alpha)$ ； $X^{q-1} - 1 = \prod_{\alpha \in F^\times} (X - \alpha)$ 。

(iii)  $F$  是多项式  $X^q - X$  和  $X^{q-1} - 1$  在  $P$  上的分裂域。■

现在我们看两个有限域在什么时候是同构的。

**定理 2.4.2** 两个有限域是同构的当且仅当它们含有相同个数的元素。

**证** 设  $F$  和  $F'$  是两个有限域，它们分别含有  $q$  和  $q'$  个元素，如果  $F \cong F'$ ，那么自然有  $q = q'$ 。现在设  $q = q'$ 。令  $\text{char } F = p$ ， $\text{char } F' = p'$ ，由 2.4.1， $q = p^f$ ， $q' = p'^{f'}$ 。则  $p^f = p'^{f'}$ 。因为  $p$  和  $p'$  都是素数，所以  $p = p'$ ， $f = f'$ ，因此， $F$  和  $F'$  各自所含的素域  $P$  和  $P'$  都是  $p$  元有限域，因而  $P \cong P'$ 。由 2.4.1， $F$  和  $F'$  分别是多项式  $X^q - X$  在  $P$  和  $P'$  上的分裂域。由 2.3.4， $F \cong F'$ 。 ■

由于这个定理，我们通常把  $q$  元有限域记作  $F_q$ 。

**定理 2.4.3** 设  $K$  是一个特征为素数  $p$  的域。 $F_q$  和  $F_{q'}$  是  $K$  的两个有限子域， $q = p^f$ ， $q' = p^{f'}$ 。那么  $F_q \subseteq F_{q'} \iff f | f'$ 。

**证**  $K$  的素域是  $p$  元有限域  $F_p$ 。

如果  $F_q \subseteq F_{q'}$ ，那么

$$f' = [F_{q'} : F_p] = [F_{q'} : F_q][F_q : F_p] = mf,$$

这里  $m = [F_{q'} : F_q]$ 。

反之，设  $f' = mf$ 。 $F_q (\subseteq K)$  是多项式  $X^q - X$  在  $F_p$  上的分裂域，所以

$$F_q = \{\alpha \mid \alpha \in K, \alpha^q - \alpha = 0\}.$$

同样，我们有

$$F_{q'} = \{\beta \mid \beta \in K, \beta^{q'} - \beta = 0\}.$$

于是

$$\begin{aligned} p^{f'} - 1 &= (p^f)^m - 1 = (p^f - 1)(p^{f(m-1)} + \\ &\quad + p^{f(m-2)} + \cdots + p^f + 1). \end{aligned}$$

如果  $\alpha \in F_q^\times$ ，则

$$\alpha^{p^{f'} - 1} - 1 = \alpha^{q - 1} - 1 = 0.$$

于是

$$\alpha^{q^{f'}-1} - 1 = \alpha^{p^{f'}-1} - 1 = 0.$$

所以  $\alpha \in F_{q^{f'}}^\times$ . 因此  $F_q^\times \subseteq F_{q^{f'}}^\times$ , 即  $F_q \subseteq F_{q^{f'}}$ . ■

现在设给定了一个素数  $p$  和一个正整数  $f$ . 是不是存在一个  $q = p^f$  个元素的有限域, 下面的定理给予肯定的回答.

**定理 2.4.4** 设  $p$  是一个素数.

(i) 给了素域  $F_p$  的一个代数闭包  $\Omega$ . 对于任意正整数  $f$ ,  $\Omega$  含有唯一的  $q = p^f$  个元素的有限域, 它是多项式  $X^q - X$  在  $F_p$  上的分裂域,

(ii) 对于  $p$  的任意幂  $q = p^f$ , 存在一个  $q$  元有限域, 如果把同构的域看作一样的, 那么这个有限域是唯一确定的.

**证** 显然 (ii) 是 (i) 和 2.4.2 的直接推论. 因此我们只需证明 (i) 成立.

令  $\Omega$  是  $F_p$  的一个代数闭包. 令  $f(X) = X^q - X \in F_p[X]$ . 因为  $f'(X) = qX^{q-1} - 1 = -1 \neq 0$ , 所以  $f(X)$  在  $\Omega$  内恰有  $q$  个两两不同的根. 令

$$F = \{\alpha \mid \alpha \in \Omega, \alpha^q - \alpha = 0\}.$$

则  $F$  含有  $q$  个元素. 设  $\alpha, \beta \in F$ . 则

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta,$$

$$(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta.$$

如果  $\beta \neq 0$ , 则

$$(\beta^{-1})^q = (\beta^q)^{-1} = \beta^{-1}.$$

所以  $F$  是  $\Omega$  的一个  $q$  元有限子域. 它由  $f(X)$  在  $\Omega$  内的全部根组成, 因而是  $f(X)$  在  $F_p$  上的分裂域, 所以是唯一确定的. ■

设  $F_q$  是一个有限域,  $q = p^f$ . 令  $e$  是任意一个自然数. 取定  $F_q$  的代数闭包  $\Omega$ . 令

$$K = \{\alpha \mid \alpha \in \Omega, \alpha^{q^e} - \alpha = 0\}.$$

则  $K$  是一个  $q^e = p^{ef}$  个元素的有限域, 并且含有  $F_q$  作为子域.

比较元素的个数，我们有

$$[K : F_q] = e.$$

于是就得到以下

**定理 2.4.5** 给定任意一个有限域  $F_q$  和任意正整数  $e$ ，存在  $F_q$  的一个  $e$  次扩域。它是一个  $q^e$  元有限域。 $F_q$  的任意两个  $e$  次扩域是同构的。■

**推论 2.4.6** 设  $F_q$  是一个  $q$  元有限域。令  $\Omega$  是  $F_q$  的一个代数闭包。则

$$\Omega = \bigcup_{f \geq 1} F_{q^f}.$$

**证** 令  $\Omega$  是  $F_q$  的一个代数闭包。对于任意正整数  $f$ ，由定理 2.4.5 的证明可以看出，在  $\Omega$  内存在  $F_q$  的唯一的  $f$  次扩域  $F_{q^f}$ 。所以  $\bigcup_{f \geq 1} F_{q^f} \subseteq \Omega$ 。

反之，设  $\alpha \in \Omega$ ，则  $F = F_q(\alpha)$  是  $F_q$  的一个有限次扩域，因而  $F = F_{q^f}$ ， $f = [F : F_q]$ 。所以  $\alpha \in F_{q^f} \subseteq \bigcup_{f \geq 1} F_{q^f}$ 。■

最后，我们证明，一个有限域的有限次扩域一定是单扩域。为此我们要进一步弄清楚有限域的乘法群的结构。先证明两个引理。

**引理 2.4.7** 设  $G$  是一个阶为  $n$  的有限群。如果对于任意正整数  $m$  来说， $G$  中满足方程  $x^m = 1$  的元素  $x$  的个数  $\leq m$ ，则  $G$  是一个循环群。

**证** 设  $d$  是  $n$  的任意一个正因数。令  $\alpha_d(G)$  表示  $G$  中阶为  $d$  的元素的个数。那么

$$\sum_{\substack{1 \leq d \leq n \\ d|n}} \alpha_d(G) = n.$$

如果  $\alpha_d(G) \neq 0$ ，那么  $G$  中存在阶为  $d$  的元素  $a$ 。令  $H$  是  $a$  所生成的循环子群。则  $H$  含有  $d$  个元素，并且对于任意  $x \in H$ ，都满足  $x^d = 1$ 。由题设的条件，我们有

$$H = \{x \in G \mid x^d = 1\}.$$

因此,  $G$  中阶为  $d$  的元素都在  $H$  内. 所以  $\alpha_d(G) = \alpha_d(H)$ . 另一方面,  $H$  是阶为  $d$  的循环群, 所以  $H$  所含的阶为  $d$  的元素等于  $\varphi(d)$ , 这里  $\varphi$  是 Euler 函数, 即  $\varphi(d)$  是小于  $d$  并且与  $d$  互素的正整数的个数. 因此, 对于  $n$  的任意正因数  $d$  来说, 或者  $\alpha_d(G) = 0$ , 或者  $\alpha_d(G) = \varphi(d)$ . 于是

$$n = \sum_{d \mid n} \alpha_d(G) \leq \sum_{d \mid n} \varphi(d) = n.$$

这样一来, 对于  $n$  的任意正因数  $d$  来说, 都有  $\alpha_d(G) = \varphi(d)$ . 特别,  $\alpha_n(G) = \varphi(n) \neq 0$ . 所以  $G$  含有阶为  $n$  的元素, 从而  $G$  是循环群.

**引理 2.4.8** 设  $F$  是一个域,  $F^\times$  是  $F$  的一切非零元素所组成的乘法群.  $F^\times$  的任意有限子群都是循环群.

**证** 设  $G$  是  $F^\times$  的一个阶为  $n$  的子群. 对于任意正整数来说, 多项式  $X^n - 1$  在  $F$  内至多有  $n$  个根, 所以  $G$  中满足  $x^n = 1$  的元素至多有  $n$  个. 于是由 2.4.7,  $G$  是循环群. ■

由 2.4.8, 立即得到

**定理 2.4.9**  $F_q$  的一切非零元素对于  $F_q$  的乘法来说作成 一个  $q-1$  阶循环群. ■

**定理 2.4.10** 有限域的有限次扩域都是单扩域.

**证** 设  $F_{q^f}$  是有限域  $F_q$  的一个  $f$  次扩域. 令  $\zeta$  是乘法群  $F_{q^f}^\times$  的一个生成元. 则

$$F_{q^f}^\times = \{1, \zeta, \dots, \zeta^{q^f-2}\}.$$

所以,  $F_{q^f} = F_q(\zeta)$ . ■

**注意** 在上面这个定理里, 取  $\zeta$  是乘法群  $F_{q^f}^\times$  的一个生成元, 自然有  $F_{q^f} = F_q(\zeta)$ . 然而反过来不一定对, 也就是说,  $F_{q^f}$  可能是对  $F_q$  添加一个不是  $F_{q^f}^\times$  的生成元而得到的单扩域.

我们看以下的例子:

例 多项式

$$f(X) = X^4 + X^3 + X^2 + X + 1$$

在  $F_2[X]$  内是不可约的. 事实上, 因为 0 和 1 都不是  $f(X)$  的根, 所以  $f(X)$  在  $F_2[X]$  内没有一次因式. 很容易证明, 在  $F_2[X]$ , 也不能分解成两个二次因式的乘积.

令  $\alpha$  是  $f(X)$  在  $F_2$  的某个扩域内的一个根. 那么  $F_2(\alpha) = F_2^4$ . 然而  $\alpha^5 - 1 = (\alpha - 1)f(\alpha) = 0$ , 所以  $\alpha^5 = 1$ , 因而  $\alpha$  不是 15 阶循环群  $F_2^{\times 4}$  的生成元.

习 题

1. 设  $p$  是一个素数. 证明, 对于任意整数  $a$  来说都有  $a^p \equiv a \pmod{p}$ .

2. 设  $p$  是一个素数,  $n > 0$ . 证明  $F_{p^n}$  中每一个元素都在  $F_{p^n}$  中有唯一的  $p$  次根.

3. 设  $K$  是  $q$  元有限域  $F_q$  的一个代数扩域. 证明  $\varphi: K \ni \alpha \mapsto \alpha^q \in K$  是  $K$  的一个自同构.

4. 构造一个有 9 个元素的域, 并且给出它的加法及乘法表.

5. 证明, 有限域不可能是代数闭域.

6. 设  $F$  是一个域,  $f(X)$  是  $F[X]$  最高次项系数为 1 的多项式, 它在  $F$  上某个分裂域中的根各不相同, 并且构成一个域. 证明  $\text{char} F = p > 0$ , 且  $f(X) = X^{p^n} - X$ , 其中  $n$  是一个正整数.

7. 设  $F_q$  是  $q$  元有限域,  $(n, q) = 1$ ,  $K$  是多项式  $X^n - 1$  在  $F_q$  上的分裂域. 证明,  $k = [K : F_q]$  是使得  $n \mid q^k - 1$  的最小正整数.

8. 设  $p$  是一个素数.  $q = p^f$ .  $f(X) \in F_q[X]$  是一个  $m$  次不

可约多项式.

(i) 证明,  $f(X) | (X^{q^n} - X) \iff m | n$ .

(ii) 令  $f_1(X), \dots, f_s(X)$  是  $F_q[X]$  中一切最高次项系数是 1 且次数是  $n$  的因数的不可约多项式. 证明

$$X^{q^n} - X = \prod_{i=1}^s f_i(X).$$

9. 找出  $F_2[X]$  的一切四次不可约多项式.

10. 设  $p$  是一个素数.  $a \in F_p$  且  $a \neq 0$ . 证明,  $X^p - X + a$  是  $F_p[X]$  中不可约多项式.

11. 设  $p$  是一个素数. 证明  $(p-1)! \equiv -1 \pmod{p}$ .

12. 构造一个满足下列条件的域  $K$ : (i)  $K$  是无限域; (ii)  $K$  是一个有限域上的代数扩域; (iii)  $K$  不是代数闭域.

13. 设  $q = p^f$ .  $p$  是一个素数, 令  $F_q^\times$  是  $F_q$  的一切非零元素所组成的乘法群. 令

$$F_q^{\times 2} = \{\alpha^2 \mid \alpha \in F_q^\times\}.$$

证明  $F_q^{\times 2}$  是  $F_q^\times$  的一个子群, 并且  $(F_q^\times : F_q^{\times 2}) = 2$ , 若  $p \neq 2$ ;

$(F_q^\times : F_q^{\times 2}) = 1$ , 若  $p = 2$ .

14. 设  $F$  是一个有限域. 记

$$F^2 + F^2 = \{\alpha^2 + \beta^2 \mid \alpha, \beta \in F\}.$$

证明,  $F^2 + F^2 = F$ .

## 2.5 可分多项式和不可分多项式

一个域  $F$  的代数扩域中每一个元素都是  $F[X]$  中一个不可约多项式的根. 在这一节里, 我们将对  $F[X]$  的不可约多项式作一些讨论.

设  $F$  是一个域.  $f(X) \in F[X]$  是一个次数大于零的多项式. 如果  $f(X)$  在  $F$  的某一个代数闭包  $\Omega$  内的根都是单根, 那么就称

$f(X)$ 是一个可分多项式；如果  $f(X)$  在  $\Omega$  内有重根，就称  $f(X)$  是一个不可分多项式。

这个定义不依赖于代数闭包的选取。事实上，设  $\Omega'$  也是  $F$  的一个代数闭包。令  $\{\alpha_1, \dots, \alpha_n\}$  和  $\{\alpha'_1, \dots, \alpha'_n\}$  分别是  $f(X)$  在  $\Omega$  和  $\Omega'$  内的全部根。则  $K = F(\alpha_1, \dots, \alpha_n) \subseteq \Omega$  和  $K' = F(\alpha'_1, \dots, \alpha'_n) \subseteq \Omega'$  都是  $f(X)$  在  $F$  上的分裂域。于是存在  $F$ -同构  $\sigma: K \rightarrow K'$ ，使得  $\sigma(\alpha_i) = \alpha'_i$ 。  $\alpha_i \neq \alpha_j \iff \alpha'_i \neq \alpha'_j$ 。不妨设  $\alpha_1, \dots, \alpha_r$  是  $f(X)$  在  $\Omega$  内一切互不相同的根，那么  $\alpha'_1, \dots, \alpha'_r$  就是  $f(X)$  在  $\Omega'$  内一切互不相同的根。因此，在  $\Omega[X]$  里，

$$f(X) = a(X - \alpha_1)^{k_1} \cdots (X - \alpha_r)^{k_r}$$

当且仅当在  $\Omega'[X]$  里，

$$f(X) = a(X - \alpha'_1)^{k_1} \cdots (X - \alpha'_r)^{k_r}.$$

**引理 2.5.1** 设  $f(X)$  是域  $F$  上一个不可约多项式。  $f(X)$  是不可分的必要且只要  $f'(X) = 0$ 。

**证**  $f(X)$  不可分  $\iff f(X)$  与  $f'(X)$  不互素。又因为  $f(X)$  不可约。所以

$$(f(X), f'(X)) \neq 1 \iff f(X) | f'(X) \iff f'(X) = 0. \quad \blacksquare$$

**引理 2.5.2** 设  $\text{char } F = p > 0$ 。  $F[X]$  的一个不可约多项式  $f(X)$  是不可分的必要且只要存在  $h(X) \in F[X]$ ，使得

$$f(X) = h(X^p)$$

**证** 设  $f(X) = \sum_{i=0}^n a_i X^i \in F[X]$  是不可约的多项式。那么

$$f'(X) = \sum_{i=1}^n i a_i X^{i-1}.$$

如果  $f(X)$  不可分。那么  $f'(X) = 0$ ，而从  $i a_i = 0$  ( $i = 1, \dots, n$ )。因此，如果  $i \not\equiv 0 \pmod{p}$ ，则  $a_i = 0$ ，令

$$h(X) = a_0 + a_p X + \cdots + a_{mp} X^m,$$

这里  $mp \leq n$ ，而  $(m+1)p > n$ 。那么



$$f(X) = h(X^p).$$

反之, 如果存在多项式  $h(X) \in F[X]$  使得  $f(X) = h(X^p)$ . 那么  $f'(X) = pX^{p-1} \cdot h'(X^p) = 0$ , 所以  $f(X)$  不可分. ■

**定理 2.5.3** 设  $f(X) \in F[X]$  是一个最高次项系数是 1 的  $n$  次不可约多项式.

(i) 如果  $\text{char} F = 0$ , 则  $f(X)$  是可分的.

(ii) 如果  $\text{char} F = p > 0$ , 那么存在唯一的非负整数  $e$  和唯一的可分的不可约多项式  $g(X) \in F[X]$ , 使得  $f(X) = g(X^{p^e})$ ; 并且  $p^e \deg(g(X)) = n$ .  $f(X)$  在  $F$  的一个代数闭包内恰有  $m$  个互不相同的根, 每一个根的重数都是  $p^e$ , 这里  $m = \deg g(X)$ .

证 设  $f(X) = \sum_{i=0}^n a_i X^i \in F[X]$ ,  $a_n = 1$ .

(i) 如果  $f(X)$  不可分, 那么由引理 2.5.1,  $f'(X) = 0$ . 从而  $ia_i = 0 \implies a_i = 0, i = 1, \dots, n$ . 于是  $f(X) = a_0 \in F$ , 这与  $f(X)$  的不可约性矛盾.

(ii) 考虑这样的  $u(X) \in F[X]$ : 存在一个非负整数  $s$ , 使得  $u(X^{p^s}) = f(X)$ . 令  $S$  是一切满足上述条件的非负整数所成的集.  $S \neq \emptyset$ , 因为  $0 \in S$ . 对于任意  $s \in S$ , 设  $u(X^{p^s}) = f(X)$ . 那么

$$n = p^s \cdot \deg(u(X)) \geq p^s.$$

所以

$$s \leq \frac{\log n}{\log p}.$$

因此  $S$  有上界, 从而是一个有限集. 令  $e$  是  $S$  中最大的数. 那么存在  $g(X) \in F[X]$ , 使得

$$f(X) = g(X^{p^e}),$$

并且对于任意非负整数  $f > e$ , 不存在  $v(X) \in F[X]$ , 使得  $f(X)$

$=v(X^{p^e})$ . 显然,  $g(X)$  的最高次项系数是 1. 我们证明,  $g(X)$  是  $F[X]$  中可分的不可约多项式. 如果

$$g(X) = g_1(X)g_2(X),$$

$g_i(X) \in F[X] (i = 1, 2)$ , 则

$$f(X) = g(X^{p^e}) = g_1(X^{p^e})g_2(X^{p^e}).$$

因为  $f(X)$  不可约, 所以  $g_1(X^{p^e})$  与  $g_2(X^{p^e})$  中必有一个是零次多项式, 从而  $g_1(X)$  与  $g_2(X)$  中必有一个是零次多项式, 所以  $g(X)$  不可约.

因为  $f(X)$  不再能表示成  $F$  上的  $X^{p^{e+1}}$  的多项式, 所以不存在  $h(X) \in F[X]$  使得  $g(X) = h(X^p)$ . 由 2.5.2,  $g(X)$  是可分的.

设  $m = \deg(g(X))$ . 则  $n = p^e m$ . 令  $\Omega$  是  $F$  的一个代数闭包. 在  $\Omega[X]$  内, 可分多项式  $g(X)$  分解成  $m$  个两两互素的一次因式的乘积:

$$g(X) = (X - \beta_1)(X - \beta_2) \cdots (X - \beta_m).$$

$\beta_i \in \Omega (1 \leq i \leq m)$ . 对于每一个  $i$ , 令  $\alpha_i$  是多项式  $X^{p^e} - \beta_i$  在  $\Omega$  内的一个根. 那么在  $\Omega[X]$  内,

$$X^{p^e} - \beta_i = X^{p^e} - \alpha_i^{p^e} = (X - \alpha_i)^{p^e},$$

并且  $\alpha_i \neq \alpha_j$ , 若  $i \neq j$ . 于是在  $\Omega[X]$  内,

$$\begin{aligned} f(X) &= g(X^{p^e}) = (X^{p^e} - \beta_1) \cdots (X^{p^e} - \beta_m) \\ &= (X - \alpha_1)^{p^e} \cdots (X - \alpha_m)^{p^e}. \end{aligned}$$

所以  $f(X)$  在  $\Omega$  中恰有  $m$  个两两不同的  $p^e$  重根  $\alpha_1, \alpha_2, \dots, \alpha_m$ . 这个事实显然不依赖于代数闭包  $\Omega$  的选取.

最后只剩下证明,  $g(X)$  和  $e$  都由  $f(X)$  唯一确定. 如果有可分的不可约多项式  $g_1(X), g_2(X)$  和非负整数  $e_1, e_2$  使得,

$$f(X) = g_1(X^{p^{e_1}}) = g_2(X^{p^{e_2}})$$

令  $m_i = \deg(g_i(X))$ ,  $i = 1, 2$ , 而  $\Omega$  是  $F$  的一个代数闭包, 那么由以上的证明, 在  $\Omega[X]$  内有

$$f(X) = g_1(X^{p^{e_1}}) = (X - \alpha_1)^{p^{e_1}} \cdots (X - \alpha_{m_1})^{p^{e_1}}.$$

$$= (X - \alpha'_1)^{p^{e_2}} \cdots (X - \alpha'_{m_2})^{p^{e_2}},$$

$\alpha_1, \dots, \alpha_{m_1} \in \Omega$  两两不同,  $\alpha'_1, \dots, \alpha'_{m_2} \in \Omega$  两两不同. 由因式分解的唯一性得出  $m_1 = m_2$ ,  $p^{e_1} = p^{e_2}$ , 从而  $e_1 = e_2$ , 并且适当对  $\alpha'_1, \dots, \alpha'_{m_2}$  编号, 可以使  $\alpha_i = \alpha'_i$ ,  $1 \leq i \leq m_1 = m_2$ , 从而  $g_1(X) = g_2(X)$ . ■

**推论 2.5.4** 在定理 2.5.3 的记号和假设下,  $f(X)$  可分当且仅当  $e = 0$ . ■

由 2.5.3, 当  $\text{char } F = p > 0$  时, 对于  $F[X]$  中每一个不可约多项式  $f(X)$ , 有唯一的可分的不可约多项式  $g(X)$  和非负整数  $e$ , 使得  $f(X) = g(X^{p^e})$ . 这个多项式  $g(X)$  的次数叫做  $f(X)$  的约化次数,  $e$  叫做  $f(X)$  的不可分指数,  $p^e$  叫做  $f(X)$  的不可分次数. 我们有

$$\deg(f(X)) = (\text{不可分次数}) \times (\text{约化次数}).$$

当  $\text{char } F = 0$  时, 任何不可约多项式都是可分的, 这时可以认为不可分指数是 0 而不可分次数是 1, 并且约化次数等于  $\deg(f(X))$ .

由 2.5.3 我们还看到, 当  $\text{char } F = p > 0$  时,  $F[X]$  中不可约多项式  $f(X)$  在它的分裂域内一切互不相同的根的个数等于  $f(X)$  的约化次数, 如果  $f(X)$  在它的分裂域中的根完全相同, 即  $f(X)$  的约化次数等于 1, 这时称  $f(X)$  是纯不可分的.

纯不可分的多项式都具有  $X^{p^n} - a (a \in F)$  的形状.

## 习 题

1. 设  $f(X)$  是域  $F$  上一个  $n$  次不可约多项式, 且  $\text{char } F \nmid n$ . 证明  $f(X)$  在  $F$  上是可分的.

2. 设  $f(X)$  是域  $F$  上一个最高次项系数为 1 的不可约多项式,  $\deg f(X) \geq 2$ . 如果  $f(X)$  在它的一个分裂域内所有的根都相同, 则  $\text{char } F = p > 0$ , 且  $f(X) = X^{p^n} - a \in F$ ,  $n \geq 1$ .

3. 设  $F$  是一个特征为  $p > 0$  的域.  $a \in F$  但  $a \notin F^p = \{b^p \mid b \in F\}$ . 证明, 对于每一个  $n > 1$ ,  $X^{p^n} - a$  是  $F$  上不可约多项式.

4. 设  $F$  是一个特征为  $p > 0$  的域,  $f(X) = \sum_{i=0}^n a_i X^i$  是  $F$  上一个可分多项式. 证明,  $g(X) = \sum_{i=0}^n a_i^p X^i$  也是  $F$  上可分多项式.

5. 设  $F_p$  是  $p$  个元素的素域,  $t$  是  $F_p$  上一个不定元,  $F = F_p(t)$ . 证明, 多项式  $X^p - t$  是  $F$  上一个纯不可分的不可约多项式.

6. 设  $F$  是一个特征为  $p > 0$  的域,  $\alpha$  是  $F$  的一个扩域  $K$  中的元素,  $\alpha^{p^e} = a \in F$  但  $\alpha^{p^{e-1}} \notin F$ . 证明,  $X^{p^e} - a$  在  $F$  上不可约.

7. 设  $k$  是一个特征为  $p > 0$  的域,  $F = k(t_1, t_2)$ ,  $t_1, t_2$  是  $k$  上不相关不定元. 证明,  $f(X) = X^{2p} + t_1 X^p + t_2$  在  $F$  上不可约. 求  $f(X)$  的约化次数和不可分指数.

## 2.6 共轭映射的个数

设  $F$  是一个域,  $\Omega$  是  $F$  的一个代数闭包.  $K$  是扩张  $\Omega/F$  的一个中间域.  $K$  到  $\Omega$  内的一个  $F$ -同态单射叫做  $K$  到  $\Omega$  内的一个  $F$ -共轭映射, 简称为  $F$ -共轭. 设  $\sigma: K \rightarrow \Omega$  是一个  $F$ -共轭. 那么  $\sigma(K)$  也是  $\Omega/F$  的一个中间域, 并且  $\sigma(K)$  与  $K$  是  $F$ -共轭的.

令  $A$  是  $K$  到  $\Omega$  内的一切  $F$ -共轭所成的集. 我们把  $A$  的基数 ( $K$  的  $F$ -共轭的个数) 记作  $\iota(K/F, \Omega)$ .

$\iota(K/F, \Omega)$  不依赖于代数闭包  $\Omega$  的选取. 事实上, 设  $\Omega$  和  $\Omega'$  都是  $F$  的代数闭包并且都包含  $K$ . 那么存在  $F$ -同构映射  $\omega: \Omega \rightarrow \Omega'$ . 令  $A$  和  $A'$  分别是  $K$  到  $\Omega$  内的  $F$ -共轭和  $K$  到  $\Omega'$  内的  $F$ -共轭所成的集. 对于任意  $\sigma \in A$ , 则  $\omega \circ \sigma \in A'$ . 反过来, 对于任意  $\sigma' \in A'$ , 则  $\omega^{-1} \circ \sigma' \in A$ . 因此,

$$A \ni \sigma \longmapsto \sigma' = \omega \circ \sigma \in A'$$

是  $A$  到  $A'$  的双射, 从而  $\iota(K/F, \Omega) = \iota(K/F, \Omega')$ . 因此, 对于代数扩张  $K/F$  来说, 我们任意取定  $F$  的一个包含  $K$  的代数闭包  $\Omega$ , 而把  $K$  到  $\Omega$  内的  $F$ -共轭的个数记作  $\iota(K/F)$ .

**定理 2.6.1** 设  $K$  是代数扩张  $L/F$  的一个中间域. 那么

$$\iota(L/F) = \iota(L/K) \iota(K/F).$$

**证** 令  $\Omega$  是  $L$  的一个代数闭包. 因为  $L/F$  是代数扩张,  $\Omega$  自然也是  $K$  和  $F$  的代数闭包. 令  $\{\lambda_i\}_{i \in I}$  是  $K$  到  $\Omega$  内的  $F$ -共轭的全体;  $\{\mu_j\}_{j \in J}$  是  $L$  到  $\Omega$  内的  $K$ -共轭的全体. 对于任意  $i \in I$  和  $j \in J$ , 由推论 2.2.6,  $\lambda_i$  可以开拓为  $\Omega$  的一个  $F$ -自同构  $\lambda'_i$ ;  $\mu_j$  可以开拓为  $\Omega$  的一个  $F$ -自同构  $\mu'_j$ . 于是  $\mu'_i \circ \mu'_j$  是  $\Omega$  的一个  $F$ -自同构. 对于  $(i, j) \in I \times J$ , 令  $\varphi_{ij}$  表示  $\lambda'_i \circ \mu'_j$  在  $L$  上的限制. 那么  $\varphi_{ij}$  是  $L$  到  $\Omega$  内的一个  $F$ -共轭. 因此, 我们只需证明以下两点:

$$1^\circ \quad (i, j) \neq (k, l) \implies \varphi_{ij} \neq \varphi_{kl};$$

2° 设  $\varphi: L \rightarrow \Omega$  是  $L$  到  $\Omega$  内的一个  $F$ -共轭. 那么存在  $(i, j) \in I \times J$ , 使得  $\varphi_{ij} = \varphi$ .

先证 1°. 如果  $\varphi_{ij} = \varphi_{kl}$ . 那么对于任意  $\alpha \in K \subseteq L$ , 都有  $\varphi_{ij}(\alpha) = \varphi_{kl}(\alpha)$ . 由于  $\alpha \in K$ , 所以

$$\varphi_{ij}(\alpha) = \lambda'_i(\mu'_j(\alpha)) = \lambda'_i(\alpha) = \lambda_i(\alpha).$$

$$\varphi_{kl}(\alpha) = \lambda'_k(\mu'_l(\alpha)) = \lambda'_k(\alpha) = \lambda_k(\alpha).$$

因此  $\lambda_i(\alpha) = \lambda_k(\alpha)$ . 这样就有  $\lambda_i = \lambda_k$ , 从而  $i = k$ .

设  $\beta \in L$ . 我们有

$$\begin{aligned} \lambda'_i(\mu'_j(\beta)) &= \lambda'_i \mu'_j((\beta)) = \varphi_{ij}(\beta) \\ &= \varphi_{kl}(\beta) = \lambda'_k(\mu'_l(\beta)) = \lambda'_k(\mu_l(\beta)). \end{aligned}$$

我们已经证明了,  $i = k$ , 又因为  $\lambda'_i$  是单射, 所以  $\mu_j(\beta) = \mu_l(\beta)$ , 因此  $\mu_j = \mu_l$ , 从而  $j = l$ , 这就证明了

$$\varphi_{ij} = \varphi_{kl} \implies (i, j) = (k, l).$$

再证 2° 成立. 设  $\varphi: L \rightarrow \Omega$  是  $L$  到  $\Omega$  内一个  $F$ -共轭. 令  $\tilde{\varphi} = \varphi|_K$ . 则  $\tilde{\varphi}$  是  $K$  到  $\Omega$  内一个  $F$ -共轭. 于是有  $i \in I$ , 使得

$\varphi = \lambda_i$ , 对于任意  $\alpha \in K$  来说,

$$\varphi(\alpha) = \tilde{\varphi}(\alpha) = \lambda_i(\alpha) = \lambda'_i(\alpha).$$

所以  $\lambda'_i{}^{-1}(\varphi(\alpha)) = \alpha$ , 即  $\lambda'_i{}^{-1} \circ \varphi$  是  $L$  到  $\Omega$  内一个  $F$ -共轭. 于是有  $j \in J$ , 使得  $\lambda'_i{}^{-1} \circ \varphi = \mu_j$ . 这样,  $\varphi = \lambda'_i \circ \mu_j$  是  $\lambda'_i \circ \mu'_j$  在  $L$  上的限制  $\varphi_{ij}$ . 定理被证明. ■

**定理 2.6.2** 设  $K = F(\alpha)$  是域  $F$  的一个单代数扩域,  $p(X)$  是  $\alpha$  在  $F$  上的最小多项式. 那么

$$i(K/F) = p(X) \text{ 的约化次数.}$$

**证** 令  $\Omega$  是  $K$  的一个代数闭包. 设  $m$  是  $p(X)$  的约化次数. 那么  $p(X)$  在  $\Omega$  内有  $m$  个互不相同的根  $\alpha_1, \dots, \alpha_m$ , 其中  $\alpha = \alpha_1$ . 由 2.2.7, 存在  $\Omega$  的  $F$ -自同构  $\omega_i$  使得  $\omega_i(\alpha) = \alpha_i$ ,  $1 \leq i \leq m$ . 令  $\varphi_i$  是  $\omega_i$  在  $K$  上的限制. 则  $\varphi_i$  是  $K$  到  $\Omega$  内的  $F$ -共轭. 当  $i \neq j$  时,  $\varphi_i(\alpha) = \alpha_i \neq \alpha_j = \varphi_j(\alpha)$ , 所以  $\varphi_i \neq \varphi_j$ . 这样,  $\varphi_1, \dots, \varphi_m$  是  $K$  到  $\Omega$  内的互不相同的  $F$ -共轭, 所以  $m \leq i(K/F)$ .

设  $\varphi$  是  $K$  到  $\Omega$  内的一个  $F$ -共轭. 令  $\alpha' = \varphi(\alpha) \in \Omega$ . 则  $p(\alpha') = p(\varphi(\alpha)) = \varphi(p(\alpha)) = 0$ . 所以  $\alpha'$  等于某一个  $\alpha_i = \varphi_i(\alpha)$ ,  $1 \leq i \leq m$ . 对于这个  $i$ , 令

$$K' = \{\beta \mid \beta \in K; \varphi(\beta) = \varphi_i(\beta)\}.$$

易证  $K'$  是  $K$  的一个子域且  $K' \supseteq F$ ,  $K' \ni \alpha$ . 所以  $K' \supseteq F(\alpha) = K$ , 从而  $K' = K$ . 因此  $\varphi = \varphi_i$ . 这就证明了  $i(K/F) \leq m$ . ■

注意到一个不可约多项式  $p(X)$  是可分的当且仅当它的约化次数等于  $p(X)$  的次数, 我们立即得到以下

**推论 2.6.4** 记号同 2.6.2. 那么

$$p(X) \text{ 可分} \iff i(K/F) = [K : F]. \quad \blacksquare$$

**定理 2.6.4** 设  $K$  是域  $F$  的一个有限次扩域. 那么

$$i(K/F) \leq [K : F].$$

**证** 因为  $[K : F] < \infty$ , 所以  $K$  是由  $F$  上有限个代数元生成的域. 设

$$K = F(\alpha_1, \dots, \alpha_n), \quad \alpha_i \in K, \quad 1 \leq i \leq n.$$

令  $F_0 = F$ ,  $F_i = F_{i-1}(\alpha_i) = F(\alpha_1, \dots, \alpha_i)$ ,  $1 \leq i \leq n$ , 我们得到一个扩域序列

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K.$$

每一个  $F_i$  是前一个域  $F_{i-1}$  的单代数扩域. 于是由 2.6.1 和 2.6.2, 我们有

$$l(K/F) = \prod_{i=1}^n l(F_i/F_{i-1}) \leq \prod_{i=1}^n [F_i : F_{i-1}] = [K : F]. \quad \blacksquare$$

## 习 题

1. 令  $\bar{Q}$  表示有理数域  $Q$  在  $C$  内的代数闭包 (即一切代数数所成的数域). 找出域  $K$  到  $\bar{Q}$  内的所有  $Q$ -同构, 其中

$$(i) \quad K = \bar{Q}(\sqrt[3]{2}); \quad (ii) \quad K = \bar{Q}(e^{2\pi i/5}).$$

## 2.7 可分扩域和不可分扩域

设  $K$  是域  $F$  的一个扩域,  $\alpha \in K$  是  $F$  上一个代数元. 如果  $\alpha$  在  $F$  上的最小多项式是可分的, 那么就称  $\alpha$  是  $F$  上一个可分元素. 类似地, 如果  $\alpha$  在  $F$  上的最小多项式是不可分或者是纯不可分的, 那么相应地就称  $\alpha$  是  $F$  上不可分或纯不可分元素.

根据这个定义, 特征为零的域上每一个代数元都是可分的. 我们看一看, 当域  $F$  的特征是一个素数  $p$  时,  $F$  上的元素在什么时候可分.

**定理 2.7.1** 设  $F$  是一个特征为  $p > 0$  的域,  $K$  是  $F$  的一个扩域,  $\alpha \in K$  是  $F$  上一个代数元. 令  $e$  是  $\alpha$  在  $F$  上最小多项式的不可分指数. 则  $\alpha^{p^e}$  是  $F$  上可分元素.

**证** 设  $p(X)$  是  $\alpha$  在  $F$  上的最小多项式. 由定理 2.5.3, 存在一个可分的不可约多项式  $g(X) \in F[X]$ , 使得  $p(X) = g(X^{p^e})$ ,  $g(\alpha^{p^e}) = f(\alpha) = 0$ . 所以  $g(X)$  是  $\alpha^{p^e}$  在  $F$  上的最小多项式, 因

而 $\alpha^{p^n}$ 是 $F$ 上可分元素。 ■

**定理 2.7.2** 设 $E$ 是域扩张 $K/F$ 的一个中间域,  $\alpha \in K$ 是 $F$ 上的代数元. 如果 $\alpha$ 在 $F$ 上可分, 那么 $\alpha$ 也在 $E$ 上可分.

**证** 令 $\alpha$ 在 $F$ 上和 $E$ 上的最小多项式分别是 $f(X)$ 和 $g(X)$ . 在 $E[X]$ 内,  $g(X) \mid f(X)$ . 因为 $f(X)$ 没有重根, 所以 $g(X)$ 也没有重根, 从而 $g(X)$ 是 $E$ 上可分多项式,  $\alpha$ 是 $E$ 上可分元素. ■

**定理 2.7.3** 设 $K$ 是特征为 $p > 0$ 的域 $F$ 上一个扩域,  $\alpha \in K$ 是 $F$ 上一个代数元.  $\alpha$ 在 $F$ 上可分必要且只要对于任意非负整数 $n$ , 都有

$$F(\alpha) = F(\alpha^{p^n}).$$

**证** 设 $\alpha$ 在 $F$ 上可分. 令 $f(X)$ 是 $\alpha$ 在 $F(\alpha^p)$ 上的最小多项式. 由2.7.2,  $f(X)$ 是 $F(\alpha^p)$ 上可分多项式, 所以没有重根. 另一方面,  $\alpha$ 是 $F(\alpha^p)$ 上多项式 $X^p - \alpha^p$ 的根. 所以在 $F(\alpha^p)[X]$ 内,  $f(X)$ 整除 $X^p - \alpha^p$ . 这样, 必须 $f(X) = X - \alpha$ , 从而 $\alpha \in F(\alpha^p)$ . 于是就得到

$$F(\alpha) = F(\alpha^p) = F[\alpha^p].$$

因此 $\alpha$ 可以表成 $\alpha^p$ 的系数属于 $F$ 的多项式:

$$\alpha = \sum_{k=0}^n a_k \alpha^{kp}, a_k \in F.$$

两边举 $p$ 次方得

$$\alpha^p = \sum_{k=0}^n a_k^p \alpha^{kp^2} \in F[\alpha^{p^2}] = F(\alpha^{p^2}).$$

所以 $F(\alpha^p) = F(\alpha^{p^2})$ . 同样的推理, 我们有

$$F(\alpha) = F(\alpha^p) = F(\alpha^{p^2}) = \cdots = F(\alpha^{p^n}) = \cdots$$

现在设 $\alpha$ 在 $F$ 上不可分. 令 $p(X)$ 是 $\alpha$ 在 $F$ 上最小多项式. 那么存在 $g(X) \in F[X]$ , 使得 $p(X) = g(X^p)$ . 所以 $g(\alpha^p) = 0$ . 于是

$$[F(\alpha^p) : F] \leq \deg(g(X)) < \deg(p(X)) = [F(\alpha) : F].$$



因而  $F(\alpha^p) \subseteq F(\alpha)$ . ■

**定理 2.7.4** 设  $K$  是特征为  $p > 0$  的域  $F$  的一个代数扩域,  $\Omega$  是  $K$  的一代数闭包. 对于  $K$  的元素  $\alpha$  来说, 下列三个条件是等价的:

- (i)  $\alpha$  是  $F$  上的纯不可分元素;
- (ii) 存在一个整数  $e \geq 0$ , 使得  $\alpha^{p^e} \in F$ ;
- (iii) 对于  $K$  到  $\Omega$  内的任意一个  $F$ -共轭  $\varphi$  来说, 都有  $\varphi(\alpha) = \alpha$ .

**证** (i)  $\implies$  (ii)  $\alpha$  在  $F$  上是纯不可分的, 所以  $\alpha$  在  $F$  上最小多项式有形状  $X^{p^e} - a$ ,  $a \in F$ ,  $e \geq 0$ . 从而  $\alpha^{p^e} = a \in F$ .

(ii)  $\implies$  (iii) 设存在整数  $e \geq 0$  使得  $\alpha^{p^e} = a \in F$ , 令  $\varphi$  是  $K$  到  $\Omega$  内的一个  $F$ -共轭映射. 则  $\varphi(\alpha^{p^e}) = \varphi(a) = a = \alpha^{p^e}$ . 于是

$$(\varphi(\alpha) - \alpha)^{p^e} = \varphi(\alpha^{p^e}) - \alpha^{p^e} = 0.$$

所以  $\varphi(\alpha) = \alpha$ .

(iii)  $\implies$  (i) 由 2.2.6,  $F(\alpha) (\subseteq K)$  到  $\Omega$  内的任意一个  $F$ -共轭  $\varphi$  可以开拓为  $\Omega$  的一个  $F$ -自同构  $\tilde{\varphi}$ .  $\tilde{\varphi}|_K$  是  $K$  到  $\Omega$  内的一个  $F$ -共轭. 因为  $\alpha \in K$ , 所以  $\varphi(\alpha) = \tilde{\varphi}(\alpha) = \alpha$ . 所以  $\varphi$  是  $F(\alpha)$  到自身的恒等自同构, 因而  $\iota(F(\alpha)/F) = 1$ . 由 2.6.2,  $\alpha$  在  $F$  上的最小多项式  $p(X)$  的约化次数等于 1, 从而  $p(X)$  是  $F$  上一个纯不可分多项式,  $\alpha$  是  $F$  上一个纯不可分元素. ■

现在我们引入可分扩域和不可分扩域的概念.

设  $K$  是域  $F$  的一个代数扩域. 如果  $K$  的每一个元素都是  $F$  上可分元素, 那么就称  $K$  是  $F$  的一个**可分扩域**. 在相反的情形, 即  $K$  中至少存在  $F$  上一个不可分元素, 就称  $K$  是  $F$  上一个**不可分扩域**.

当  $\text{char } F = 0$  时,  $F$  的任何代数扩域都是  $F$  上可分扩域. 当  $\text{char } F = p > 0$  时, 也存在  $F$  上可分扩域, 因为我们有

**定理 2.7.5** 有限域的代数扩域是可分的.

**证** 设  $F$  是一个有限域,  $K$  是  $F$  的一个代数扩域. 设  $\alpha \in K^\bullet$  则  $F(\alpha)$  是  $F$  的一个有限次扩域, 因而也是一个有限域, 设  $F(\alpha) = F_\sigma$ . 那么  $\alpha$  是可分多项式  $X^q - X \in F[X]$  的根. 因此, 作为  $X^q - X$  的一个因式,  $\alpha$  在  $F$  上的最小多项式也是可分的. 从而  $\alpha$  是  $F$  上可分元素. ■

让我们看一个不可分扩域的例子.

**例** 设  $k$  是一个特征为  $p > 0$  的域,  $t$  是  $k$  上一个不定元. 令  $F = k(t)$ . 设  $n$  是一个正整数且  $p \mid n$ , 多项式  $f(X) = X^n - t \in F[X]$  是不可约的. 事实上,  $t$  是环  $k[t]$  的一个不可约元素, 由 Eisenstein 判断法,  $f(X)$  不能分解成为系数在  $k[t]$  内的两个次数都低于  $n$  的多项式的积. 因而在  $k[t]$  的商域  $F = k(t)$  上不可约. 又因为  $f'(X) = nX^{n-1} = 0$ , 所以  $f(X)$  是  $F$  上不可分的多项式. 令  $\Omega$  是  $F$  的一个代数闭包,  $\alpha \in \Omega$  是  $f(X)$  的一个根. 由于  $\alpha$  在  $F$  上最小多项式  $f(X)$  不可分, 所以  $\alpha = t^{1/n}$  是  $F$  上不可分元素, 因而  $K = F(\alpha)$  是  $F$  的一个  $n$  次不可分扩域.

**定理 2.7.6** 设  $K$  是域  $F$  的一个扩域. 对于  $K$  来说, 下列三个条件是等价的:

- (i)  $K$  是  $F$  的有限次可分扩域;
- (ii)  $K = F(\alpha_1, \dots, \alpha_n)$ , 每一个  $\alpha_i \in K$  都是  $F$  上可分元素,  $i = 1, \dots, n$ ;
- (iii)  $\iota(K/F) = [K : F] < \infty$ .

**证** (i)  $\implies$  (ii)  $K$  是  $F$  的有限次扩域, 于是由 2.1.2,  $K = F(\alpha_1, \dots, \alpha_n)$ , 每一个都是  $F$  上代数元. 又因为  $K$  是  $F$  上可分扩域, 所以每一个  $\alpha_i$  ( $1 \leq i \leq n$ ) 都是  $F$  上可分元素.

(ii)  $\implies$  (iii)  $K = F(\alpha_1, \dots, \alpha_n)$ , 每一个  $\alpha_i$  都是  $F$  上可分元素. 仍由 2.1.2,  $[K : F] < \infty$ . 令  $F_0 = F$ ,  $F_i = F(\alpha_1, \dots, \alpha_i)$ ,  $i = 1, \dots, n$ , 我们有以下的扩域序列:

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K, \quad F_i = F_{i-1}(\alpha_i), \quad 1 \leq i \leq n.$$

由 2.7.2, 每一个  $\alpha_i$  都是  $F_{i-1}$  上的可分元素. 再由 2.6.3,

$$\iota(F_i/F_{i-1}) = [F_i : F_{i-1}], \quad 1 \leq i \leq n.$$

于是由 2.6.1,

$$\iota(K/F) = \prod_{i=1}^n \iota(F_i/F_{i-1}) = \prod_{i=1}^n [F_i : F_{i-1}] = [K : F].$$

(iii)  $\implies$  (i) 我们只需证明,  $K$  的每一个元素都是  $F$  上可分元素. 设  $\alpha \in K$ . 由 2.6.4,

$$\iota(F(\alpha)/F) \leq [F(\alpha) : F], \quad \iota(K/F(\alpha)) \leq [K : F(\alpha)].$$

这样一来就有

$$\begin{aligned} [K : F] &= \iota(K/F) = \iota(K/F(\alpha)) \iota(F(\alpha)/F) \\ &\leq [K : F(\alpha)] [F(\alpha) : F] = [K : F]. \end{aligned}$$

因此必须  $\iota(F(\alpha)/F) = [F(\alpha) : F]$  (同时也有  $\iota(K/F(\alpha)) = [K : F(\alpha)]$ ). 由 2.6.3,  $\alpha$  是  $F$  上可分元素. ■

**推论 2.7.7** 设  $K = F(S)$ ,  $S \subseteq K$  是由域  $F$  上一些可分元素所组成的集. 则  $K$  是  $F$  的可分扩域.

**证** 由 2.1.3, 可以归结为是有限集的情形, 而后一情形正是定理 2.7.6. ■

**定理 2.7.8** 设  $K$  是域  $F$  的一个代数扩域,  $E$  是扩张  $K/F$  的一个中间域.

$$K/F \text{ 可分} \iff K/E \text{ 和 } E/F \text{ 都可分}.$$

**证** 设  $K/F$  可分, 由 2.7.2 推出  $K/E$  可分; 又  $E \subseteq K$ , 所以  $E/F$  自然可分.

反之, 设  $\alpha \in K$ . 令

$$g(X) = X^m + \beta_1 X^{m-1} + \cdots + \beta_m, \quad \beta_i \in E.$$

是  $\alpha$  在  $E$  上的最小多项式. 那么  $g(X)$  是  $E$  上可分多项式. 又根据假设和 2.7.6,  $E' = F(\beta_1, \dots, \beta_m) \subseteq E$  是  $F$  的有限次可分扩域, 所以

$$\iota(E'/F) = [E' : F] < \infty.$$

另一方面,  $g(X)$  是  $E'[X]$  的一个不可约多项式, 所以  $g(X)$  也是  $\alpha$  在  $E'$  上的最小多项式. 于是由 2.6.3,

$$[E'(\alpha)/E'] = [E'(\alpha) : E'].$$

于是就有

$$\begin{aligned} [E'(\alpha)/F] &= [E'(\alpha)/E'] [E'/F] = [E'(\alpha) : E'] [E' : F] \\ &= [E'(\alpha) : F] < \infty. \end{aligned}$$

所以  $E'(\alpha) = F(\beta_1, \dots, \beta_m, \alpha)$  是  $F$  的一个有限次可分扩域, 从而  $\alpha$  是  $F$  上可分元素. 这就证明了  $K/F$  是可分扩张. ■

**定理 2.7.9** 设  $K$  是域  $F$  的一个代数扩域. 令  $S$  是  $K$  中在  $F$  上可分元素的全体. 则  $F \subseteq S$ , 并且  $S$  是  $K$  的一个在  $F$  上可分的子域.

**证** 对于  $F$  的任意元素  $a$ ,  $a$  在  $F$  上的最小多项式  $X - a$  自然是  $F$  上可分多项式, 所以  $F \subseteq S$ .

设  $\alpha, \beta \in S$ . 由 2.7.6,  $F(\alpha, \beta)$  是  $F$  的可分扩域, 所以  $\alpha - \beta, \alpha\beta$  都是  $F$  上可分元素, 从而属于  $S$ ; 如果  $\beta \neq 0$ , 则  $\beta^{-1} \in S$ , 所以  $S$  是  $K$  的一个子域.  $S$  自然是  $F$  的可分扩域. ■

设  $K$  是域  $F$  的一个代数扩域. 由  $K$  中一切在  $F$  上可分元素所组成的子域  $S$  叫做  $F$  在  $K$  内的可分闭包.  $S$  显然是  $K$  的一切在  $F$  上可分的子域中最大者.

域  $F$  在  $F$  的一个代数闭包内的可分闭包简称作  $F$  的可分闭包.

显然, 域  $F$  的一个代数扩域  $K$  是可分的充要条件是  $F$  在  $K$  内的可分闭包与  $K$  重合.

## 习 题

1. 设  $F$  是一个特征为  $p > 0$  的域,  $K$  是  $F$  的一个有限次扩域且  $p \nmid [K : F]$ . 证明,  $K$  是  $F$  的可分扩域.
2. 设  $F$  是一个特征为  $p > 0$  的域,  $K = F(\alpha, \beta)$ , 这里  $\alpha$  是  $F$  上  $n$  次可分元素而  $\beta$  是  $F$  上  $p$  次不可分元素. 求  $[K : F]$ .

3. 设  $F$  是一个特征为  $p > 0$  的域. 多项式  $f(X) \in F[X]$  叫做一个  $p$ -多项式, 如果  $f(X)$  具有形状  $X^{p^m} + a_1 X^{p^{m-1}} + \cdots + a_m X$ . 证明, 一个  $p$ -多项式的根组成其分裂域的加法群的一个有限子群, 且每一个根都有相同的重数  $p^e$ ,  $e$  是一个非负整数.

4. 设  $F$  是一个特征为  $p > 0$  的域,  $a \in F$ . 证明:

(i)  $f(X) = X^p - X - a$  没有重根;

(ii)  $f(X)$  在  $F[X]$  中不可约必要且只要对于任何  $c \in F$  来说,  $a \neq c^p - c$ .

5. 设  $K$  是域  $F$  的一个扩域,  $\alpha, \beta \in K$ , 其中  $\alpha$  是  $F$  上一个可分元素而  $\beta$  是  $F$  上一个纯不可分元素. 证明,  $F(\alpha, \beta) = F(\alpha + \beta)$ . 如果  $\alpha\beta \neq 0$ , 则  $F(\alpha, \beta) = F(\alpha + \beta) = F(\alpha\beta)$ .

6. 设  $K$  是域  $F$  的一个代数扩域,  $K_i$  是  $K$  中一切在  $F$  上纯不可分的元素所成的集. 证明,  $K_i$  是  $K/F$  的一个中间域.

7. 设  $K, L$  都是域扩张  $M/F$  的中间域, 证明:

(i) 如果  $K/F$  是可分扩张, 则  $KL/L$  是可分扩张;

(ii) 如果  $K/F, L/F$  都是可分扩张, 则  $KL/F$  也是可分扩张.

8. 设  $K$  是域  $F$  的一个可分扩域,  $\Omega$  是  $K$  的一个代数闭包. 证明, 对于  $K$  的元素  $\alpha$  来说, 以下两条件是等价的:

(i)  $\alpha \in F$ ; (ii) 对于  $K$  到  $\Omega$  内的任意  $F$ -同构  $\sigma$  来说, 都有  $\sigma(\alpha) = \alpha$ .

9. 设  $K$  是域  $F$  的一个代数扩域,  $\text{char } F = p > 0$ . 证明:

(i) 如果  $K$  是  $F$  上可分扩域, 则对于任意正整数  $e$  来说, 都有  $K = FK^{p^e}$ ;

(ii) 如果  $[K : F] < \infty$ , 且  $K = FK^p$ , 则  $K$  是  $F$  上可分扩域.

## 2.8 纯不可分扩域 可分次数和不可分次数

设  $K$  是域  $F$  的一个代数扩域. 如果  $F$  在  $K$  内的可分闭包与  $F$  重合, 那么就称  $K$  是  $F$  的一个纯不可分扩域. 相应地, 称  $K/F$  是一个纯不可分扩张. 这个条件相当于说,  $K \setminus F$  的每一个元素都是  $F$  上的不可分元素.

**定理 2.8.1** 设  $K$  是域  $F$  的一个代数扩域,  $S$  是  $F$  在  $K$  内的可分闭包. 那么  $K$  是  $S$  上纯不可分扩域.

**证** 令  $S'$  是  $S$  在  $K$  内的可分闭包, 则  $S'$  是  $S$  的一个可分扩域. 又  $S$  是  $F$  的可分扩域, 所以  $S'$  是  $F$  的可分扩域, 从而  $S' \subseteq S$ . 这样,  $S' = S$ , 即  $K$  是  $S$  的纯不可分扩域. ■

根据纯不可分域扩张的定义, 与定理 2.7.4 完全平行, 我们有

**定理 2.8.2** 设  $F$  是一个特征为  $p > 0$  的域. 对于  $F$  的一个代数扩域  $K$  来说, 下列三个条件是等价的:

- (i)  $K$  是  $F$  的纯不可分扩域;
- (ii) 对于任意  $\alpha \in K$ , 存在整数  $e \geq 0$ , 使得  $\alpha^{p^e} \in F$ ;
- (iii)  $\iota(K/F) = 1$ . ■

**推论 2.8.3** 设  $E$  是代数域扩张  $K/F$  的一个中间域.  $K/F$  是纯不可分扩张必要且只要  $K/E$  和  $E/F$  都是纯不可分扩张.

**证** 因为  $\iota(K/F) = \iota(K/E)\iota(E/F)$ , 所以,  $\iota(K/F) = 1$  必要且只要  $\iota(K/E) = \iota(E/F) = 1$ . 于是由 2.8.2 就得到这个推论. ■

**推论 2.8.4** 设  $F$  是一个特征为  $p > 0$  的域,  $K$  是  $F$  的一个有限次纯不可分扩域. 则

- (i)  $[K : F] = p^f$ ,  $f$  是一个非负整数;
- (ii) 存在整数  $e \geq 0$ , 使得

$$K^{p^e} = \{\alpha^{p^e} \mid \alpha \in K\}$$

是  $F$  的一个子域.

证 因为  $K$  是  $F$  的有限次扩域, 所以存在  $F$  上代数元  $\alpha_1, \dots, \alpha_n \in K$ , 使得

$$K = F(\alpha_1, \dots, \alpha_n).$$

因为  $K$  是  $F$  的纯不可分扩域, 由 2.8.2, 对于每一个  $\alpha_i$ , 存在整数  $e_i \geq 0$ , 使得  $\alpha_i^{p^{e_i}} = a_i \in F$ , 所以  $\alpha_i$  是多项式  $f_i(X) = X^{p^{e_i}} - a_i$

$\in F[X]$  的根. 令  $F_0 = F$ ,  $F_i = F(\alpha_1, \dots, \alpha_i) = F_{i-1}(\alpha_i)$ , 那么  $\alpha_i$  在  $F_{i-1}$  上的最小多项式  $g_i(X)$  整除  $f_i(X)$ , 所以  $[F_i : F_{i-1}] = \deg(g_i(X))$  也是  $p$  的一个幂. 于是

$$[K : F] = \prod_{i=1}^n [F_i : F_{i-1}] = p^f.$$

这就证明了 (i) 成立.

(ii) 对于任意整数  $e \geq 0$ ,  $K \ni \alpha \mapsto \alpha^{p^e} \in K$  是  $K$  到  $K$  内的一个同态单射, 所以

$$K^{p^e} = \{\alpha^{p^e} \mid \alpha \in K\}$$

是  $K$  的一个子域. 我们证明, 对于足够大的  $e$ , 将有  $K^{p^e} \subseteq F$ .

用证明 (i) 时所引入的记号, 我们有扩域序列

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K,$$

$F_i = F_{i-1}(\alpha_i)$ . 我们证明, 对于每个  $i$ ,  $1 \leq i \leq n$ , 存在  $e_i \geq 0$ , 使得  $F_i^{p^{e_i}} \subseteq F_{i-1}$ . 如果这一事实被证明, 那么取  $e = e_1 + e_2 + \dots + e_n$ , 则  $K^{p^e} \subseteq F$ , 因此, 问题就归结为证明以下论断:

设  $K = F(\alpha)$ ,  $\alpha$  是  $F$  上一个纯不可分元素. 那么存在整数  $e \geq 0$ , 使得  $K^{p^e} \subseteq F$ .

为了证明这个论断, 我们注意到, 由 2.8.2, 存在整数  $e \geq 0$ , 使得  $\alpha^{p^e} = a \in F$ .  $K = F(\alpha)$  的任意元素  $\gamma$  总可以表示成

$$\gamma = \sum_{i=1}^m a_i \alpha^i, \quad a_i \in F.$$

于是

$$\gamma^{p^e} = \sum_{i=0}^m a_i^{p^e} (\alpha^{p^e})^i = \sum_{i=0}^m a_i^{p^e} \alpha^i \in F.$$

所以  $K^{p^e} \subseteq F$ . ■

在这一节的最后，我们引入可分次数和不可分次数的概念。

设  $K$  是域  $F$  的一个代数扩域， $S$  是  $F$  在  $K$  内的可分闭包。  $S$  在  $F$  上的次数  $[S : F]$  叫做  $K$  在  $F$  上的可分次数；  $K$  在  $S$  上的次数  $[K : S]$  叫做  $K$  在  $F$  上的不可分次数。

我们分别用  $[K : F]_s$  和  $[K : F]_i$  来表示  $K$  在  $F$  上的可分次数和不可分次数，因此，当  $[K : F] < \infty$  时，我们有

$$[K : F] = [K : F]_s [K : F]_i.$$

并且有

$$K/F \text{ 可分} \iff [K : F] = [K : F]_s.$$

令  $\Omega$  是  $K$  的一个代数闭包。我们知道，当  $[K : F] < \infty$  时， $K$  到  $\Omega$  内的  $F$ -共轭的个数  $\iota(K/F)$  小于或等于域次数  $[K : F]$  (2.6.4)。下面的定理明说  $\iota(K/F)$  与可分次数  $[K : F]_s$  的关系。

**定理 2.8.5** 设  $K$  是域  $F$  的一个有限次扩域。那么

$$\iota(K/F) = [K : F]_s.$$

**证** 令  $S$  是  $F$  在  $K$  内的可分闭包，则  $K$  是  $S$  的纯不可分扩域。由 2.8.2， $\iota(K/S) = 1$ 。所以

$$\iota(K/F) = \iota(K/S) \iota(S/F) = \iota(S/F).$$

另一方面， $S$  是  $F$  的有限次可分扩域，由 2.7.6，

$$[K : F]_s = \iota(S/F).$$

因此， $\iota(K/F) = [K : F]_s$ . ■

**定理 2.8.6** 设  $K$  是域  $F$  的一个有限次扩域， $E$  是  $K/F$  的



一个中间域。那么

$$[K : F]_s = [K : E]_s [E : F]_s;$$

$$[K : F]_i = [K : E]_i [E : F]_i.$$

证 由 2.8.5, 我们有

$$\begin{aligned} [K : F]_s &= \iota(K/F) = \iota(K/E) \iota(E/F) \\ &= [K : E]_s [E : F]_s. \end{aligned}$$

然而  $[K : F] = [K : E][E : F]$ . 由此得出

$$[K : F]_i = [K : E]_i [E : F]_i. \quad \blacksquare$$

### 习 题

1. 写出定理 2.8.2 的证明.

2. 设  $K$  是域  $F$  的一个扩域,  $S$  是  $F$  在  $K$  内的可分闭包,  $P$  是  $K$  内一切在  $F$  上纯不可分元素所成的集,  $E$  是  $K/F$  的一个中间域. 证明:

(i)  $K$  在  $E$  上是纯不可分的  $\iff S \subseteq E$ ;

(ii) 如果  $K$  在  $E$  上是可分的, 则  $P \subseteq E$ ;

(iii) 如果  $E \cap S = F$ , 则  $E \subseteq P$ .

3. 设  $F$  是一个特征为  $p > 0$  的域,  $\alpha$  是  $F$  上一个代数元. 证明, 如果  $F(\alpha)$  在  $F$  上是纯不可分的, 则  $[F(\alpha) : F] = p^e$ ,  $e$  是一个正整数.

4. 设  $K = F_p(X, Y)$  是  $p$  元素域  $F_p$  上不相关不定元  $X, Y$  的有理分式域, 令  $F = F_p(X^p, Y^p - Y)$ . 证明,  $[K : F] = p^2$ . 确定  $F$  在  $K$  内的可分闭包  $S$ , 并且求出  $[K : F]_s$  及  $[K : F]_i$ .

5. 设  $K = F_p(X, Y)$  是  $F_p$  上不相关不定元  $X, Y$  的有理分式域,  $F = F_p(X^p - X, Y^p - Y)$ . 证明:

(i)  $K$  是  $F$  的  $p^2$  次可分扩域;

(ii)  $K$  中在  $F$  上纯不可分的元素都在  $F$  内.

## 2.9 完备域

我们已经对于可分扩域和不可分扩域的性质作了一些讨论. 现在提出这样的问题: 给了一个域  $F$ , 在什么条件下,  $F$  的每一个代扩域都是可分的? 当  $\text{char } F = 0$  时, 这是不成为问题的, 因为特征为 0 的域的任何代数扩域总是可分的. 问题主要出在  $\text{char } F = p > 0$  的情形. 先给出以下定义.

一个域  $F$  说是**完备的**, 如果  $F$  的每一个代数扩域都是可分的. 这相当于说,  $F[X]$  的每一个不可约多项式都是可分的. 事实上, 如果  $F[X]$  的每一个不可约多项式都可分, 那么  $F$  上每一个代数元在  $F$  上的最小多项式是可分的, 因而  $\alpha$  是  $F$  上可分元素. 反之, 设  $f(X)$  是  $F[X]$  的一个不可约多项式, 令  $\alpha$  是  $f(X)$  的一个根 (在  $F$  的某一代数闭包内). 那么  $\alpha$  在  $F$  上的最小多项式  $p(X)$  是可分的, 而  $f(X)$  与  $p(X)$  至多相差  $F$  中一个非零常数因子, 所以  $f(X)$  也是可分的.

由这个定义, 注意到 2.7.5, 我们立即得到

**定理 2.9.1** (i) 特征为 0 的域是完备域.

(ii) 有限域是完备域. ■

**定理 2.9.2** 完备域的代数扩域还是完备域.

**证** 设  $K$  是完备域  $F$  的一个代数扩域. 令  $L$  是  $K$  的任意一个代数扩域.  $L$  也是  $F$  的代数扩域. 所以  $L$  是  $F$  的可分扩域. 再由 2.7.8,  $L$  是  $K$  的可分扩域, 所以  $K$  是完备的. ■

现在设  $F$  是一个域,  $\text{char } F = p > 0$ , 令  $\Omega$  是  $F$  的一个代数闭包. 对于任意非负整数  $v$  定义

$$F^{p^v} = \{x^{p^v} \mid x \in F\};$$

$$F^{p^{-v}} = \{\alpha \mid \alpha \in \Omega, \alpha^{p^v} \in F\}.$$

容易验证,  $F^{p^v}$  和  $F^{p^{-v}}$  都是  $\Omega$  的子域, 并且有

$$F \supseteq F^p \supseteq F^{p^2} \supseteq \dots$$

$$F \subseteq F^{p^{-1}} \subseteq F^{p^{-2}} \subseteq \cdots \subseteq \Omega.$$

约定

$$F^{p^{-\infty}} = \bigcup_{v \geq 0} F^{p^{-v}},$$

则  $F^{p^{-\infty}}$  也是  $\Omega$  的一个子域.

**定理 2.9.3** 设  $F$  是一个域,  $\text{char } F = p > 0$ . 对于  $F$  来说, 下列五个条件等价:

- (i)  $F$  是完备域;
- (ii)  $F[X]$  的每一个不可约多项式都是可分的;
- (iii)  $F^{p^{-\infty}} = F$ ;
- (iv)  $F^{p^{-1}} = F$ ;
- (v)  $F^p = F$ .

**证** (i) 和 (ii) 显然等价. 我们只证条件 (i), (iii), (iv), (v) 的等价性.

(i)  $\implies$  (iii) 如果  $F^{p^{-\infty}} \neq F$ , 那么存在整数  $v > 0$ , 使得有  $\alpha \in F^{p^{-v}}$  但  $\alpha \notin F$ , 而  $\alpha^{p^v} \in F$ . 所以  $\alpha$  是  $F$  上纯不可分元素 (2.7.4). 于是  $F$  的代数扩域  $F(\alpha)$  是  $F$  的一个不可分扩域.

(iii)  $\implies$  (iv)  $F \subsetneq F^{p^{-1}} \implies F \subsetneq F^{p^{-\infty}}$ .

(iv)  $\implies$  (v)  $F^{p^{-1}} = F \iff$  对于任意  $a \in F$ , 都有  $b \in F$ , 使得  $a = b^p \in F^p \iff F^p = F$ .

(v)  $\implies$  (i) 如果  $F$  不是完备域, 那么存在  $\alpha \in \Omega$ ,  $\alpha$  在  $F$  上不可分. 令  $f(X) \in F[X]$  是  $\alpha$  在  $F$  上的最小多项式, 则  $f(X)$  不可分. 于是存在  $g(X) \in F[X]$  使得  $f(X) = g(X^p)$ . 令

$$g(X) = \sum_{i=0}^m b_i X^i, \quad b_i \in F.$$

因为  $F^p = F$ , 所以每一个系数都可以写成  $b_i = a_i^p$  的形式,  $a_i \in F$  ( $0 \leq i \leq m$ ). 于是

$$f(X) = g(X^p) = \sum_{i=0}^m b_i X^{ip}$$

$$= \sum_{i=0}^m a_i^p X^{ip} = \left( \sum_{i=1}^m a_i X^i \right)^p$$

这与  $f(X)$  的不可约性相违. ■

**推论 2.9.4** 设  $F$  是一个特征为  $p > 0$  的域. 则  $F^{p^{-\infty}}$  是完备域.

**证** 设  $\alpha \in F^{p^{-\infty}}$ . 那么存在一个整数  $v \geq 0$  使得  $\alpha \in F^{p^{-v}}$ . 令  $\beta$  是多项式  $X^p - \alpha$  的一个根 (在  $F^{p^{-\infty}}$  的某一代数闭包内). 则

$$\beta \in F^{p^{-(v+1)}} \subseteq F^{p^{-\infty}}, \text{ 且 } \beta^p = \alpha.$$

所以

$$(F^{p^{-\infty}})^p = F^{p^{-\infty}}.$$

由 2.9.3, (v),  $F^{p^{-\infty}}$  是完备的. ■

## 习 题

1. 设  $K$  是域  $F$  的一个有限次扩域. 证明,  $K$  是完备域必要且只要  $F$  是完备域.

2. 设  $F$  是一个特征为  $p > 0$  的非完备域,  $a \in F$  但  $a \notin F^p$ . 证明, 多项式  $X^{p^e} - a$  在  $F[X]$  中不可约, 这里  $e$  是一个非负整数.

3. 设  $F$  是一个特征为  $p > 0$  的域,  $t$  是  $F$  上一个超越元. 证明  $F(t)$  不是完备域.

4. 设  $F$  是一个特征为  $p > 0$  的域. 证明:

(i)  $F^{p^{-\infty}}$  是包含  $F$  的最小完备域;

(ii) 对于每一个正整数  $v$  来说,  $F^{p^{-v}}$  与  $F$  同构, 但  $F^{p^{-\infty}}$  不一定与  $F$  同构.

## 2.10 本原元素定理

我们证明域的有限次可分扩域的一个重要的性质来结束这一章.

先证明关于单代数扩域的一个性质.

**定理 2.10.1** 令  $K$  是域  $F$  的一个扩域. 那么  $K$  是  $F$  的一个有限次单扩域必要且只要  $K/F$  只有有限个中间域.

**证** 如果  $K$  是  $F$  的有限次单扩域, 那么存在  $K$  的一个元素  $\alpha$ , 使得  $K = F(\alpha)$ , 并且  $\alpha$  是  $F$  上的代数元. 令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式. 设  $E$  是  $K/F$  的一个中间域, 那么  $\alpha$  在  $E$  上也是代数的. 令  $f_E(X) \in E[X]$  是  $\alpha$  在  $E$  上的最小多项式. 我们有  $f_F(X) = f(X)$ ,  $f_K(X) = X - \alpha$ .  $f_E(X)$  是由中间域  $E$  唯一确定的. 令

$$\mathfrak{M} = \{E \mid E \text{ 是 } K/F \text{ 的中间域}\}.$$

$$\mathfrak{N} = \{f_E(X) \mid f_E(X) \text{ 是 } \alpha \text{ 在 } E \text{ 上的最小多项式, } E \in \mathfrak{M}\}.$$

那么  $E \mapsto f_E(X)$  是  $\mathfrak{M}$  到  $\mathfrak{N}$  的满射. 我们证明, 这个映射是双射. 事实上, 设  $E_1, E_2 \in \mathfrak{M}$ . 如果

$$f_{E_1}(X) = f_{E_2}(X) = g(X).$$

令  $L = E_1 \cap E_2$ . 则  $g(X) \in E_1[X] \cap E_2[X] = L[X]$ .  $g(X)$  是  $E_1[X]$  的不可约多项式, 自然也是  $L[X]$  的不可约多项式. 因为  $g(\alpha) = 0$ , 所以  $g(X)$  是  $\alpha$  在  $L$  上最小多项式:  $g(X) = f_L(X)$ . 另一方面,  $K = F(\alpha)$  而  $F \subseteq L \subseteq E_i \subseteq K$ , 所以

$$K = L(\alpha) = E_i(\alpha), \quad i = 1, 2.$$

又  $[K : E_i] = \deg(f_{E_i}(X)) = \deg(g(X)) = [K : L]$ , 所以

$$[E_i : L] = [K : L] / [K : E_i] = 1, \quad i = 1, 2.$$

于是  $E_1 = L = E_2$ . 这就证明了映射  $E \mapsto f_E(X)$  是集  $\mathfrak{M}$  到  $\mathfrak{N}$  集的双射.

$\mathfrak{N}$  是有限集, 因为对于任意中间域  $E$ , 多项式  $f_E(X)$  整除  $f(X)$ , 而  $f(X)$  的最高次项系数是 1 的非常数因式只有有限多个. 因此  $\mathfrak{N}$  是有限集.

反之, 设  $K/F$  只有有限个中间域. 我们首先证明,  $K$  是  $F$  的代数扩域. 事实上, 如果  $K$  含有  $F$  上的一个超越元  $x$ , 那么  $x^2$

也是  $F$  上超越元, 并且  $F(x) \subsetneq F(x^2)$ . 这样一来,  $K/F$  含有无限多个中间域

$$K \supsetneq F(x) \subsetneq F(x^2) \subsetneq F(x^4) \subsetneq \cdots \subsetneq F(x^{2^n}) \subsetneq \cdots \subsetneq F.$$

与题设矛盾.

其次,  $K$  是  $F$  上有限个代数元生成的扩域. 因为如果不然的话, 必定存在一个扩域的无限序列,

$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \cdots, \alpha_n) \subsetneq \cdots \subsetneq K.$$

这又与题设矛盾.

这样,  $K$  是  $F$  上有限个代数元生成的扩域, 因而是  $F$  的有限次扩域.

我们证明  $K$  是  $F$  的单扩域. 如果  $F$  是有限域, 那么由 2.4.10,  $K$  是  $F$  的单扩域. 现在设  $F$  是无限域. 对于任意  $\alpha \in K$ , 我们有

$$[F(\alpha) : F] \leq [K : F] < \infty.$$

又因为  $K/F$  只有有限中间域, 所以

$$\{[F(\alpha) : F] \mid \alpha \in K\}$$

是自然数的有限集, 因此存在  $\theta \in K$ , 使得对于任意  $\alpha \in K$  都有

$$[F(\theta) : F] \geq [F(\alpha) : F].$$

考虑  $K$  中任意元素  $\beta$ . 对于任意  $c \in F$ , 令

$$E_c = F(\beta + c\theta).$$

则  $F \subseteq E_c \subseteq K$ . 由假设, 这样的  $E_c$  只有有限多个. 然而  $F$  含有无限多个元素, 因此必存在  $c_1, c_2 \in F, c_1 \neq c_2$ , 而  $E_{c_1} = E_{c_2} = E$ . 因为  $\beta + c_1\theta, \beta + c_2\theta \in E$ , 所以  $\theta \in E$ . 于是

$$F(\theta) \subseteq E = F(\beta + c_1\theta).$$

所以

$$[F(\theta) : F] \leq [F(\beta + c_1\theta) : F].$$

由  $\theta$  的取法, 必须等号成立, 从而

$$F(\theta) = E = F(\beta + c_1\theta).$$

由此得出,  $\beta = (\beta + c_1\theta) - c_1\theta \in F(\theta)$ . 这样一来,  $K$  中任意

元素  $\beta$  都属于  $F(\theta)$ , 从而  $K = F(\theta)$ . ■

我们现在证明以下的所谓本原元素定理.

**定理 2.10.2** 设  $K = F(\alpha_1, \dots, \alpha_s, \beta)$  是域  $F$  的一个代数扩域, 其中  $\alpha_1, \dots, \alpha_s$  都是  $F$  上的可分元素. 那么  $K$  是  $F$  的一个单扩域.

**证** 如果  $F$  是有限域, 那么由 2.4.10, 定理成立. 设  $F$  是无限域. 先看  $s=1$  的情形. 这时  $K = F(\alpha, \beta)$ ,  $\alpha, \beta$  是  $F$  上代数元且  $\alpha$  在  $F$  上可分. 令  $\Omega$  是  $K$  的一个代数闭包. 令

$$m = \iota(K/F) = [K : F]_s,$$

设  $\sigma_i : K \longrightarrow \Omega$  ( $1 \leq i \leq m$ ) 是  $K$  到  $\Omega$  内的一切互不相同的  $F$ -共轭映射. 那么当  $i \neq j$  时, 或者  $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ , 或者  $\sigma_i(\beta) \neq \sigma_j(\beta)$ . 因为  $F$  是无限域, 所以对于一切数对  $(i, j)$ ,  $1 \leq i \leq m$ ,  $i \neq j$ , 总可以找到  $F$  的一个元素  $c$ , 使得

$$(\sigma_i(\alpha) - \sigma_j(\alpha)) + c(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0.$$

令  $\theta = \alpha + c\beta$ . 则  $\theta \in K$ , 所以  $F \subseteq F(\theta) \subseteq K$ . 由  $c$  的取法可知当  $i \neq j$  时,  $\sigma_i(\theta) \neq \sigma_j(\theta)$ . 因此,  $\sigma_i$  在  $F(\theta)$  上的限制  $\sigma_i|_{F(\theta)}$  ( $i=1, 2, \dots, m$ ) 是  $F(\theta)$  到  $\Omega$  内的  $m$  个互不相同的  $F$ -共轭. 于是

$$[K : F]_s = \iota(K/F) \leq \iota(F(\theta)/F) = [F(\theta) : F]_s.$$

另一方面, 因为  $F \subseteq F(\theta) \subseteq K$ , 所以

$$[F(\theta) : F]_s \leq [K : F]_s.$$

因此必须

$$[F(\theta) : F]_s = [K : F]_s.$$

这就是说,  $F$  在  $F(\theta)$  内的可分闭包与  $F$  在  $K$  内的可分闭包重合. 令  $S$  表示这个可分闭包. 那么  $\alpha \in S \subseteq F(\theta)$ , 从而  $\beta = c^{-1}(\theta - \alpha) \in F(\theta)$ . 这样一来,  $K = F(\alpha, \beta) \subseteq F(\theta)$ , 即  $K = F(\theta)$ .

设  $s \geq 2$ .  $K = F(\alpha_1, \dots, \alpha_s, \beta)$ , 其中  $\alpha_1, \dots, \alpha_s$  都是  $F$  上可分元素. 由归纳法假设, 存在  $\gamma \in K$  使得  $K' = F(\alpha_1, \dots, \alpha_{s-1}, \beta) = F(\gamma)$ . 于是  $K = K'(\alpha_s) = F(\alpha_s, \gamma)$ , 这就归结到前一个情

形。因此存在  $\theta \in K$  使  $K = F(\theta)$ . ■

由这个定理, 立即得出以下两个推论:

**推论 2.10.3** 设  $K$  是域  $F$  的一个有限次可分扩域, 则  $K$  是  $F$  上的单扩域. ■

**推论 2.10.4** 设  $K$  是域  $F$  的一个有限次可分扩域, 则  $K/F$  只有有限个中间域. ■

由本原元素定理, 我们可以对于代数闭包用一个较弱的条件来刻画.

**定理 2.10.5** 设  $K$  是域  $F$  的一个代数扩域. 对于  $K$  来说, 以下两个条件是等价的:

- (i)  $K$  是  $F$  的代数闭包;
- (ii)  $F[X]$  的每一个次数大于零的多项式在  $K$  中有一个根.

**证** (i)  $\implies$  (ii) 是明显的.

(ii)  $\implies$  (i) 令  $\Omega$  是  $K$  的一个代数闭包. 则  $\Omega$  自然也是  $F$  的代数闭包. 我们证明  $\Omega = K$ . 分两个情形讨论.

(a)  $\text{char } F = p > 0$ . 设  $\alpha \in \Omega$ . 令  $f(X)$  是  $\alpha$  在  $F$  上最小多项式. 于是存在非负数  $e$  和  $F$  上一个不可约的可分多项式  $g(X)$  使得  $f(X) = g(X^{p^e})$ .  $g(X)$  在  $\Omega[X]$  内分解成一次因式乘积:

$$g(X) = \prod_{i=1}^m (X - \beta_i),$$

这里  $\beta_1, \dots, \beta_m$  是  $\Omega$  中两两不同的可分元素. 于是由 2.10.2,  $L = F(\beta_1, \dots, \beta_m)$  是  $F$  上的单扩域, 即存在  $\theta \in L$  使得  $L = F(\theta)$ . 然而

$$0 = f(\alpha) = g(\alpha^{p^e}) = \prod_{i=1}^m (\alpha^{p^e} - \beta_i),$$

所以  $\alpha^{p^e}$  必定等于某一个  $\beta_i$ , 从而  $\alpha^{p^e} \in L$ .



令  $h(X)$  是  $\theta$  在  $F$  上的最小多项式, 则  $h(X^{p^e})$  是  $F[X]$  的一个次数大于零的多项式. 由 (ii),  $h(X^{p^e})$  在  $K$  里有一个根  $\gamma$ . 令  $\theta_1 = \gamma^{p^e}$ , 则  $h(\theta_1) = 0$ . 由 2.2.7, 存在  $\Omega$  的一个  $F$ -自同构  $\omega$ , 使得  $\omega(\theta) = \theta_1$ , 从而  $L = F(\theta)$  与  $F(\theta_1)$  是  $F$ -共轭的. 然而  $L$  是  $g(X)$  在  $F$  上的分裂域, 因而是  $F$  的正规扩域, 因此  $L = F(\theta_1)$ . 这样就得出  $\alpha^{p^e} = \beta_i \in L = F(\theta_1)$ . 所以

$$\alpha^{p^e} = \sum_{j=0}^s a_j \theta_1^j, \quad a_j \in F.$$

由 (ii), 每一个多项式  $X^{p^e} - a_j \in F[X]$  在  $K$  里有一个根  $\alpha_j, 0 \leq j \leq s$ , 因此

$$\alpha^{p^e} = \sum_{j=0}^s a_j \theta_1^j = \sum_{j=0}^s \alpha_j^{p^e} (\gamma^{p^e})^j = \left( \sum_{j=0}^s a_j \gamma^j \right)^{p^e}.$$

所以

$$\alpha = \sum_{j=0}^s \alpha_j \gamma^j \in K.$$

这就证明了  $\Omega \subseteq K$  从而  $K = \Omega$  是  $F$  的代数闭包.

(b) 设  $\text{char } F = 0$ . 设  $\alpha \in \Omega$ . 令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式. 则  $f(X)$  在  $\Omega[X]$  中可以分解成一次因式的乘积:

$$f(X) = \prod_{i=1}^n (X - \alpha_i), \quad \alpha_i \in \Omega.$$

并且当  $i \neq j$  时,  $\alpha_i \neq \alpha_j$ . 令  $L = F(\alpha_1, \dots, \alpha_n)$ . 则  $\alpha \in L$ . 由 2.10.2,  $L = F(\theta)$ ,  $\theta$  是  $L$  中一个元素, 令  $h(X)$  是  $\theta$  在  $F$  上的最小多项式. 由 (ii),  $h(X)$  在  $K$  里有一个根  $\theta_1$ . 又因为  $L$  是  $f(X)$  在  $F$  上的分裂域, 因而是正规扩域. 由此推出  $L = F(\theta_1)$ . 这样就有  $\alpha \in L = F(\theta_1) \subseteq K$ , 从而  $K = \Omega$ . ■

由于  $F[X]$  中每一个次数大于零的多项式都是  $F[X]$  的一些不可约多项式的乘积, 我们立即得到

**推论 2.10.6** 对于域  $F$  的一个代数扩域  $K$  来说, 以下两个条件是等价的:

- (i)  $K$  是  $F$  的代数闭包;
- (ii)  $F[X]$  的每一个不可约多项式在  $K$  中有一个根. ■

## 习 题

1. 设  $K$  是域  $F$  的一个  $n$  次单扩域. 证明,  $K/F$  的中间域的个数至多等于  $2^n - 1$ .

2. 设  $K$  是域  $F$  的有限次可分扩域,  $\Omega$  是  $K$  的代数闭包,  $\alpha \in K$ . 证明以下两条件是等价的:

- (i)  $\alpha$  是  $K$  在  $F$  上一个本原元素, 即  $K = F(\alpha)$ ;
- (ii) 在  $\Omega$  内,  $\alpha$  在  $F$  上的共轭元素的个数等于  $[K : F]$ .

3. 令  $k$  是一个特征为  $p > 0$  的域,  $F = k(t_1, t_2)$  是  $k$  上不相关不定元  $t_1, t_2$  的有理分式域.  $\Omega$  是  $F$  的一个代数闭包,  $\alpha_1, \alpha_2$  分别是  $X^p - t_1$  和  $X^p - t_2 \in F[X]$  在  $\Omega$  内的根. 令  $K = F(\alpha_1, \alpha_2)$ . 证明:

- (i)  $[K : F] = p^2$ , 且  $K/F$  是不可分扩张;
- (ii) 对于任意  $\alpha \in K$ , 都有  $[F(\alpha) : F] \leq p$ ;
- (iii)  $K$  不是  $F$  上的单扩域;
- (iv)  $K/F$  有无限多个中间域.

4. 设  $K$  是域  $F$  上一个可分扩域. 证明, 如果  $K$  中每一个元素在  $F$  上的最小多项式的次数都有一个共同的上界  $N$ , 那么  $K/F$  是有限次扩张, 且  $[K : F] \leq N$ .

### 第三章 Galois理论

Galois 理论主要是在一个特定的域扩张  $K/F$  的中间域所组成的集与  $K$  的  $F$ -自同构群的子群所组成的集之间建立了一个双射. 这样就使得域论问题的研究可以归为群论问题, 从而得到域论中一些较为深刻的结果.

#### 3.1 Galois 扩域

设  $K$  是一个域. 令  $\text{Aut}(K)$  表示  $K$  的一切自同构所组成的集. 设  $\sigma, \tau \in \text{Aut}(K)$ , 那么合成映射  $\sigma \circ \tau$  仍是  $K$  的一个自同构. 我们定义  $\sigma$  与  $\tau$  的积  $\sigma\tau = \sigma \circ \tau$ , 即对于任意  $\alpha \in K$ ,

$$\sigma\tau(\alpha) = \sigma(\tau(\alpha)).$$

这样定义的乘法自然满足结合律. 恒等自同构  $1_K$  是单位元. 又  $K$  的每一个自同构  $\sigma$  有逆  $\sigma^{-1}$ , 并且  $\sigma^{-1}$  也是  $K$  的自同构. 这样,  $\text{Aut}(K)$  对于如上定义的乘法作成一个群, 称为  $K$  的全体自同构群.

设  $F$  是域  $K$  的一个子域. 令

$$G(K/F) = \{\sigma \in \text{Aut}(K) \mid \sigma(a) = a, \forall a \in F\}.$$

$G(K/F)$  就是  $K$  的一切  $F$ -自同构所组成的集. 它是  $\text{Aut}(K)$  的一个子群, 称为  $K$  的  $F$ -自同构群

反过来设  $G$  是  $\text{Aut}(K)$  的一个子群. 令

$$K^G = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}.$$

那么  $K^G$  是  $K$  的一个子域, 称为群  $G$  的固定域.

现在给定一个域  $K$ . 设  $F$  是  $K$  的一个子域.  $H$  是  $\text{Aut}(K)$  的一个子群. 记  $G(F) = G(K/F)$  是  $K$  的  $F$ -自同构群;  $K^H$  是子群

$H$  的固定域. 又记  $1 = 1_K$ . 我们有以下事实:

1.  $F \subseteq K^{G(F)}$ .
2.  $H \subseteq G(K^H)$ .
3.  $F_1, F_2$  是  $K$  的子域, 且  $F_1 \subseteq F_2$ , 则  $G(F_1) \supseteq G(F_2)$ ;  
 $G(K) = \{1\}$ .
4.  $H_1, H_2$  是  $\text{Aut}(K)$  的子群, 且  $H_1 \subseteq H_2$  则  $K^{H_1} \supseteq K^{H_2}$ ;  
 $K^{(1)} = K$ .
5.  $G(F) = G(K^{G(F)})$ .

这些事实的证明都是非常容易的. 我们只证 5.

由 1,  $F \subseteq K^{G(F)}$ . 再由 3,

$$G(F) \supseteq G(K^{G(F)}).$$

另一方面, 由 2,

$$G(F) \subseteq G(K^{G(F)}).$$

所以

$$G(F) = G(K^{G(F)}).$$

**例 1** 设  $F = \mathbb{Q}$  是有理数域,  $K = \mathbb{Q}(\sqrt[3]{2})$ . 那么  $G(F) = G(K/F) = \{1\}$ , 从而  $K^{G(F)} = K$ .

**例 2** 设  $F = F_p(x)$  是  $p$  元有限域  $F_p$  上不定元  $x$  的有理分式域;  $K = F(x^{1/p})$ . 那么  $K$  是  $F$  的一个纯不可分扩域. 所以  $K$  只有唯一的  $F$ -自同构——恒等自同构  $1$ . 因此  $G(F) = \{1\}$ , 而  $K^{G(F)} = K \cong F$ .

以上两个例子告诉我们, 1 中的包含关系可能是真包含关系. 在 Galois 理论中, 主要是讨论这样的域扩张  $K/F$ , 其中  $F = K^{G(F)}$ .

**定理 3.1.1** 设  $K$  是域  $F$  的一个代数扩域. 对于  $K$  来说, 下列三个条件是等价的:

- (i)  $K$  是  $F$  的一个可分正规扩域;
- (ii)  $F = K^{G(F)}$ ;

(iii) 存在  $G(F)$  的一个子群  $G$ , 使得  $F = K^G$ .

证 (i)  $\Rightarrow$  (ii) 我们只需证明  $K^{G(F)} \subseteq F$ . 设  $\alpha \in K$  但  $\alpha \notin F$ . 令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式. 由 (i),  $f(X)$  在  $K[X]$  内分解成两两互素的一次因子的乘积:

$$f(X) = \prod_{i=1}^n (X - \alpha_i),$$

这里  $\alpha_i \in K$ , 且  $\alpha_1, \alpha_2, \dots, \alpha_n$  两两不同. 令  $\alpha_1 = \alpha$ . 因为  $\alpha \notin F$ , 所以  $n = \deg(f(X)) > 1$ . 所以有  $\alpha_2 \in K$ ,  $\alpha_2 \neq \alpha$ , 由 2.3.3, 存在  $\sigma \in G(F)$  使得  $\sigma(\alpha) = \alpha_2 \neq \alpha$ . 所以  $\alpha \notin K^{G(F)}$ .

(ii)  $\Rightarrow$  (iii) 由 (ii), 取  $G = G(F)$  即可.

(iii)  $\Rightarrow$  (i) 设有  $G(F)$  的一个子群  $G$ , 使得  $F = K^G$ . 对于任意  $\alpha \in K$ , 令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式. 那么对于任意  $\sigma \in G \subseteq G(F)$ , 我们有

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0.$$

所以  $\sigma(\alpha)$  也是  $f(X)$  在  $K$  内的一个根. 然而  $f(X)$  在  $K$  内只有有限个根, 所以

$$\Sigma_\sigma = \{\sigma(\alpha) \mid \sigma \in G\}$$

是有限集, 设  $\Sigma_\sigma = \{\alpha_1, \dots, \alpha_n\}$ ,  $\alpha_i \neq \alpha_j$ , 若  $i \neq j$ . 那么对于任意  $\tau \in G$ ,  $\tau(\alpha_1), \dots, \tau(\alpha_n)$  仍是  $f(X)$  在  $K$  内两两不同的根, 从而

$$\Sigma_\sigma = \{\tau(\alpha_1), \dots, \tau(\alpha_n)\}.$$

令

$$g(X) = \prod_{i=1}^n (X - \alpha_i).$$

$g(X)$  的系数是  $\alpha_1, \dots, \alpha_n$  的对称多项式, 所以在  $\tau$  的作用下保持不动, 从而属于  $K^G = F$ . 这样  $g(X) \in F[X]$ , 因为  $\alpha \in \Sigma_\sigma$ , 所以  $g(\alpha) = 0$ , 因而  $g(X)$  可以被  $\alpha$  在  $F$  上的最小多项式  $f(X)$  整除. 于是在  $K[X]$  里,  $f(X)$  可以分解成两两互素的一次因式

的乘积。由 2.3.2,  $K$  是  $F$  的一个正规扩域。  $f(X)$  是  $F$  上可分多项式。所以  $\alpha$  是  $F$  上可分元素, 因而  $K$  是  $F$  的一个可分正规扩域。 ■

**定义** 设  $K$  是域  $F$  的一个代数扩域, 如果  $K$  满足 3.1.1 中三个等价的条件之一, 就称  $K$  是  $F$  的一个 Galois 扩域; 这时  $K/F$  称为一个 Galois 扩张;  $K$  的  $F$ -自同构群  $G(F)=G(K/F)$  称  $K/F$  的 Galois 群。

**定理 3.1.2** 设  $K$  是域  $F$  的一个扩域。对于  $K$  来说, 以下两个条件是等价的:

- (i)  $K$  是  $F$  的有限次 Galois 扩域;
- (ii)  $K$  是  $F[X]$  中一些可分的不可约多项式  $f_1(X), \dots, f_s(X)$  的幂的乘积

$$f(X) = \prod_{i=1}^s f_i(X)^{e_i}, e_i \geq 1, 1 \leq i \leq s,$$

在  $F$  上的一个分裂域。

**证** (i)  $\Rightarrow$  (ii)  $K$  是  $F$  上有限次正规扩域。由 2.3.5,  $K$  是  $F[X]$  中一个多项式  $f(X)$  在  $F$  上的分裂域。可设  $f(X)$  最高次项系数是 1。在  $F[X]$  内,  $f(X)$  分解成不可约多项式幂的乘积:

$$f(X) = \prod_{i=1}^s f_i(X)^{e_i},$$

$f_i(X) \in F[X]$  是最高次项系数为 1 的不可约多项式,  $e_i \geq 1, i=1, \dots, s$ 。因为在  $K[X]$  内,  $f(X)$  可以分解成为一次因式的积, 所以每一个  $f_i(X)$  在  $K[X]$  内也可以分解成为一次因式的积:

$$f_i(X) = \prod_{j=1}^{n_i} (X - \alpha_{ij}),$$

$\alpha_{ij} \in K, 1 \leq j \leq n_i, 1 \leq i \leq s$ 。  $f_i(X)$  是  $K$  的元素  $\alpha_{ij}$  在  $F$  上的

最小多项式. 因为  $K$  是  $F$  的可分扩域, 所以  $\alpha_i$  是  $F$  上可分元素, 即  $f_i(X)$  是  $F$  上可分多项式,  $1 \leq i \leq s$ .

(ii)  $\implies$  (i) 我们有

$$f(X) = a \prod_{i=1}^n (X - \alpha_i),$$

$a \in F, \alpha_i \in K, 1 \leq i \leq n; K = F(\alpha_1, \dots, \alpha_n)$ . 由 2.3.5,  $K$  是  $F$  的有限次正规扩域. 因为每一个  $\alpha_i$  都是  $F[X]$  中某一个可分的不可约多项式的根, 所以  $\alpha_i$  是  $F$  上可分元素. 由 2.7.6,  $K$  是  $F$  上一个可分扩域, 这样,  $K$  就是  $F$  上一个有限次 Galois 扩域. ■

因为特征为 0 的域的每一扩域都是可分的, 所以立即得到

**推论 3.1.3** 设  $\text{char} F = 0$ .  $K$  是域  $F$  的一个有限次 Galois 扩域当且仅当  $K$  是  $F[X]$  的某一个多项式的分裂域. ■

**定理 3.1.4** 设  $K$  是域  $F$  的一个有限次扩域. 对于  $K$  来说, 以下两条件是等价的:

- (i)  $K$  是  $F$  的一个 Galois 扩域;
- (ii) 群  $G(K/F)$  的阶等于域次数  $[K : F]$ .

**证** (i)  $\implies$  (ii). 令  $\Omega$  是  $K$  的一个代数闭包. 因为  $K$  是  $F$  的 Galois 扩域, 所以是正规扩域. 因此对于  $K$  的任意  $F$ -共轭  $\sigma : K \rightarrow \Omega$  来说, 都有  $\sigma(K) = K$ , 从而  $\sigma \in G(K/F)$ . 因为  $K$  是  $F$  的可分扩域, 所以

$$|G(K/F)| = \iota(K/F) = [K : F].$$

(ii)  $\implies$  (i) 令  $E = K^{G(K/F)}$ . 则  $F \subseteq E \subseteq K$ , 由 3.1.1(ii),  $K$  是  $E$  的 Galois 扩域. 由本节开始时所述的事实 5, 我们有

$$G(K/E) = G(K/F).$$

这样一来, 可以对于 Galois 扩张  $K/E$  应用 (i)  $\implies$  (ii). 于是我们有

$$|G(K/F)| = |G(K/E)| = [K : E] \leq [K : F].$$

另一方面, 我们已知  $|G(K/F)| = [K : F]$ . 这样就有  $[K : E]$

$=[K:F]$ , 从而  $E=F$ . 即  $K$  是  $F$  的 Galois 扩域. ■

**定理 3.1.5** 设  $K$  是域  $F$  的一个有限次可分扩域;  $\Omega$  是  $F$  的一个包含  $K$  的代数闭包. 那么存在  $\Omega$  的一个子域  $L$ , 它满足以下条件:

- (i)  $F \subseteq K \subseteq L \subseteq \Omega$ , 并且  $L/F$  是有限次 Galois 扩张;
- (ii) 如果  $N \subseteq \Omega$  是  $F$  的一个包含  $K$  的 Galois 扩域, 那么  $L \subseteq N$ .

**证** 因为  $K$  是  $F$  的有限次可分扩域, 所以由 2.10.3,  $K = F(\alpha)$  是  $F$  的一个单扩域.  $\alpha$  在  $F$  上最小多项式  $f(X)$  是可分的. 令  $L \subseteq \Omega$  是  $f(X)$  在  $F$  上的分裂域. 由 3.1.2,  $L$  是  $F$  的有限次 Galois 扩域, 并且

$$F \subseteq K \subseteq L \subseteq \Omega.$$

设  $N \subseteq \Omega$  是  $F$  的任意一个 Galois 扩域, 且  $N \supseteq K$ . 则  $\alpha \in K \subseteq N$ . 因为  $N$  是  $F$  上正规扩域, 所以由 2.3.2,  $f(X)$  在  $N[X]$  中可以分解成为一次因式的积:

$$f(X) = \prod_{i=1}^n (X - \alpha_i), \quad \alpha_i \in N.$$

因此  $L = F(\alpha_1, \dots, \alpha_n) \subseteq N$ .

**注1.** 由(ii)立即推出  $L$  是唯一确定的. ■

2. 设  $[K:F] = n$ . 则  $G = G(L/F)$  是集合  $\{\alpha_1, \dots, \alpha_n\}$  上的一个置换群. 设  $\sigma \in G$ ,  $\sigma(\alpha_i) = \alpha_{v_i}$ ,  $1 \leq i \leq n$ . 因为  $L = F(\alpha_1, \dots, \alpha_n)$ , 所以

$$G \ni \sigma \mapsto \begin{pmatrix} 1 & 2 & \cdots & n \\ v_1 & v_2 & \cdots & v_n \end{pmatrix} \in S_n$$

是一个群同态单射, 这里  $S_n$  表示  $n$  次对称群. 因而  $G$  同构于  $S_n$  的一个子群. 于是  $[L:F] = |G|$  是  $n!$  的一个因数.

由定理 3.1.5, 对于域  $F$  的一个有限次可分扩域  $K (\subseteq \Omega)$ , 由条件(i), (ii)所唯一确定的有限次 Galois 扩域  $L$  称为扩张



$K/F$ 的 Galois 闭包.

**定理 3.1.6** 设  $E$  是域扩张  $K/F$  的一个中间域. 如果  $K/F$  是 Galois 扩张, 则  $K/E$  也是 Galois 扩张.

证  $K$  是  $F$  上可分扩域, 所以也是  $E$  上可分扩域. 设  $K'$  是  $K$  在  $E$  上任意一个共轭域. 那么在  $K$  和  $K'$  的一个共同的扩域  $M$  内, 存在  $K$  到  $K'$  的一个  $E$ -同构  $\varphi$ . 因为  $E \supseteq F$ , 所以  $\varphi$  也是一个  $F$ -同构. 因而  $K$  与  $K'$  是  $F$ -共轭的. 因为  $K$  是  $F$  的正规扩域, 所以  $K' = \varphi(K) = K$ . 因此  $K$  也是  $E$  的正规扩域. 这样,  $K/E$  是可分正规扩张, 从而是 Galois 扩张. ■

**注意**  $E/F$  一般不是 Galois 扩张. 参看下一节例 4 和例 5.

**定理 3.1.7** 设  $K$  是域  $F$  的一个正规扩域;  $G = G(K/F)$  是  $K$  的一切  $F$ -自同构所成的群;  $K^G$  是  $G$  在  $K$  中的固定域. 又设  $K_s$  是  $F$  在  $K$  内的可分闭包,  $K_i$  是  $K$  中一切在  $F$  上纯不可分元素的集. 那么

(i)  $K^G = K_i$ , 从而  $K_i$  是  $K$  的一个包含  $F$  的子域;

(ii)  $K$  是  $K_i$  上的 Galois 扩域,  $K/K_i$  的 Galois 群就是  $G$ ;

(iii)  $K = K_s K_i$ ,  $K_s \cap K_i = F$ .

证 令  $\Omega$  是  $K$  的一个代数闭包.

(i) 由 2.7.4 (iii),  $\alpha \in K_i$  当且仅当对于  $K$  到  $\Omega$  内的任意一个  $F$ -共轭  $\varphi$  来说, 都有  $\varphi(\alpha) = \alpha$ . 然而  $K$  是  $F$  的正规扩域, 因此  $K$  到  $\Omega$  的每一个  $F$ -共轭  $\varphi$  都是  $K$  的  $F$ -自同构, 即  $\varphi \in G(K/F) = G$ . 因此  $\alpha \in K_i$  当且仅当对于任意  $\varphi \in G$ , 都有  $\varphi(\alpha) = \alpha$ , 也就是说, 当且仅当  $\alpha \in K^G$ . 所以  $K^G = K_i$ .

(ii) 由 (i), 我们有

$$G(K/K_i) = G(K_i) = G(K^G) = G.$$

(iii)  $K/K_s$  是纯不可分扩张. 由 2.8.3,  $K/K_s K_i$  也是纯不可分扩张. 然而由 (ii),  $K/K_i$  是可分扩张, 所以由 2.7.8,

$K/K_s, K_i$  也是可分扩张。因此必须  $K = K_s K_i$ 。

最后,  $K_s \cap K_i$  中任意元素  $\alpha$  既在  $F$  上可分又在  $F$  上不可分, 所以  $\alpha \in F$ , 从而  $K_s \cap K_i = F$ . ■

**推论 3.1.8** 设  $K$  是域  $F$  上一个有限次正规扩域。那么

$$[K : K_i] = [K_s : F], [K : K_s] = [K_i : F].$$

**证** 由 3.1.7,  $K/K_i$  是有限次 Galois 扩张, 它的 Galois 群是  $G(K/K_i) = G(K/F)$ 。于是由 3.1.4 和 2.8.5,

$$[K : K_i] = |G(K/F)| = i(K/F) = [K_s : F].$$

于是

$$\begin{aligned} [K : K_s] &= [K : F] / [K_s : F] = [K : F] / [K : K_i] \\ &= [K_i : F]. \end{aligned} \quad \blacksquare$$

最后我们再给出有关扩域的合成域的一个定理。

**定理 3.1.9** 设  $K$  是域  $F$  的一个 Galois 扩域,  $L$  是  $F$  的任意扩域, 并且假设  $K$  和  $L$  都被包含在某一个共同的扩域内。则

- (i)  $KL$  是  $L$  的 Galois 扩域;
- (ii) 如果  $[K : K \cap L] < \infty$ , 则

$$[KL : L] = [K : K \cap L],$$

并且

$$G(KL/L) \cong G(K/K \cap L).$$

**证** (i) 因为  $K$  是  $F$  的可分扩域, 所以  $K$  的每一个元素也在  $L \supseteq F$  上可分。由 2.7.7,  $KL = L(K)$  是  $L$  上可分扩域。

令  $\sigma$  是  $KL$  的任意一个  $L$ -共轭。则  $\sigma$  在  $K$  上的限制  $\sigma|_K$  自然是  $K$  的一个  $F$ -共轭。因为  $K/F$  是正规扩张, 所以  $\sigma(K) = K$ 。因为  $KL$  的每一个元素都是  $K$  和  $L$  的元素的积的组合, 所以  $\sigma(KL) = KL$ 。因此  $KL$  是  $L$  的正规扩域。

这样,  $KL$  是  $L$  的 Galois 扩域。

(ii) 令  $E = K \cap L$ 。由 3.1.6,  $K/E$  也是有限次 Galois 扩张, 因而是有限次可分扩张。于是由 2.10.3, 存在  $\alpha \in K$ , 使

得  $K = E(\alpha)$ . 设  $f(X)$  是  $\alpha$  在  $E$  上的最小多项式. 因为  $K$  是  $E$  的正规扩域, 所以由 2.3.2, 在  $K[X]$  内,

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n),$$

$\alpha_i \in K, 1 \leq i \leq n, \alpha = \alpha_1$ . 另一方面,  $\alpha$  也是  $L$  上代数元, 且  $KL = LE(\alpha) = L(\alpha)$ . 令  $g(X)$  是  $\alpha$  在  $L$  上的最小多项式. 那么在  $L[X]$  内,  $g(X) | f(X)$ . 所以  $g(X)$  的根都是  $f(X)$  的根, 因而属于  $K$ . 于是  $g(X)$  的系数作为根的初等对称多项式, 都属于  $K$ , 从而属于  $E = K \cap L$ . 这样一来就必须有  $f(X) = g(X)$ . 因此

$$[KL : L] = \deg(g(X)) = \deg(f(X)) = [K : E].$$

现在设  $\sigma \in G(KL/L)$ . 那么  $\sigma|_K$  自然使  $E = K \cap L$  的元素保持不动, 所以  $\sigma|_K \in G(K/E)$ . 这样,

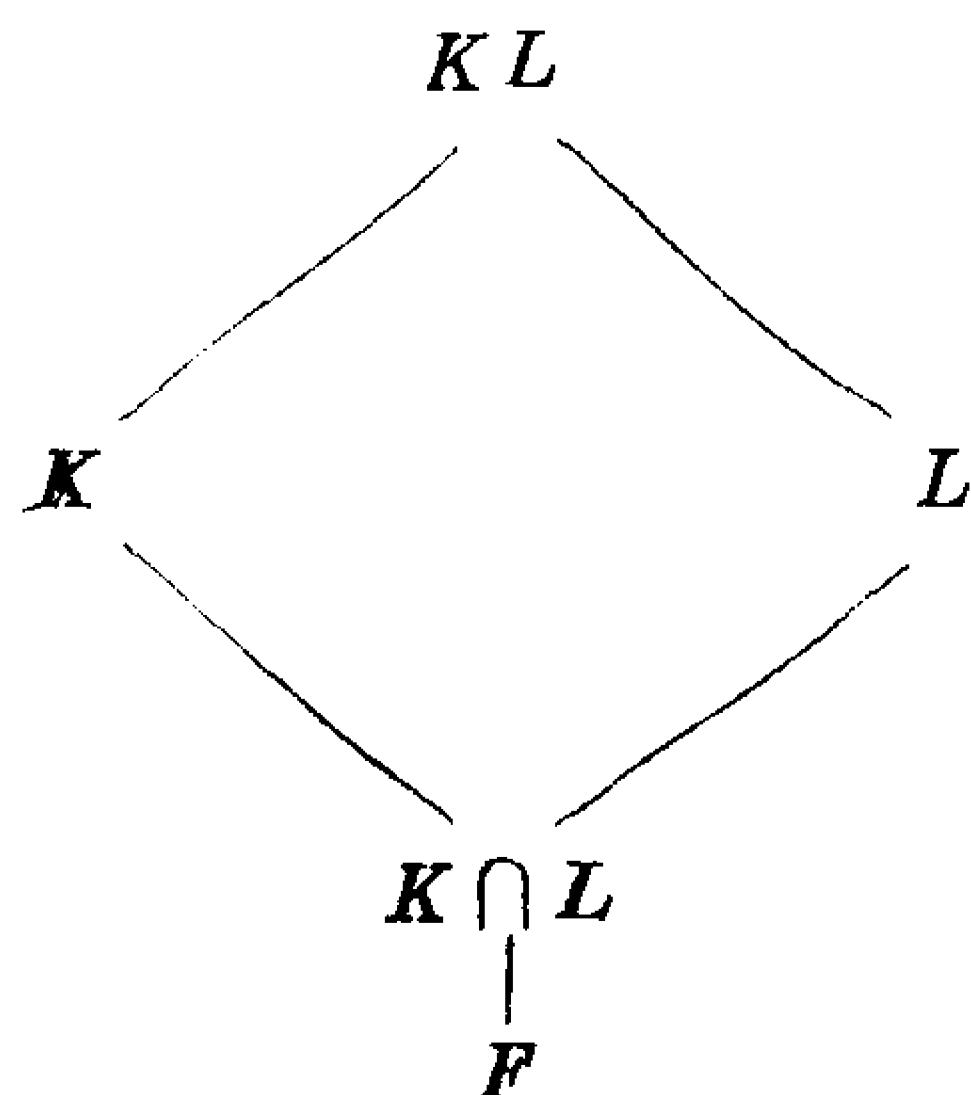
$$\theta : G(KL/L) \ni \sigma \mapsto \sigma|_K \in G(K/E)$$

是群  $G(KL/L)$  到群  $G(K/E)$  的同态映射. 如果  $\sigma \in G(KL/L)$  而  $\sigma|_K = 1_K$ , 则显然  $\sigma = 1_{KL}$ . 因而  $\theta$  是单射. 最后再由 3.1.4 和上面所证明的事实, 我们有

$$|G(KL/L)| = [KL : L] = [K : E] = |G(K/E)|.$$

所以  $G(KL/L) \cong G(K/E) = G(K/K \cap L)$ . ■

定理 3.1.9 可以用左边的图来示意.



注意, 在上面定理的证明里,  $K/F$  是 Galois 扩张这一条件是必要的. 当  $K$  和  $L$  都不是  $F$  的 Galois 扩域时, 定理一般不成立. 例如令  $K = \mathbb{Q}(\sqrt[3]{2})$ ,  $L = \mathbb{Q}(\zeta \sqrt[3]{2})$ ,  $\zeta = e^{2\pi i/3}$ . 则  $K \cap L = \mathbb{Q}$ ,  $KL = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ , 我们有  $[KL : \mathbb{Q}] = 6$ ,  $[L : \mathbb{Q}] = 3$ , 以所  $[KL : L] = 2$ .

然而  $[K : K \cap L] = [K : \mathbb{Q}] = 3$ . (参看 3.2, 例 4.)

## 习 题

1. 设  $m, n$  是不含平方因子的不同的整数,  $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ , 证明,  $K/\mathbb{Q}$  是 Galois 扩张. 确定 Galois 群  $G(K/\mathbb{Q})$ .

2. 设  $E = \mathbb{Q}(\sqrt{2})$ ,  $K = \mathbb{Q}(\sqrt[4]{2})$ . 证明  $K/E$  和  $E/\mathbb{Q}$  都是 Galois 扩张.  $K/\mathbb{Q}$  是不是 Galois 扩张?

3. 设  $k$  是一个特征为  $p > 0$  的域,  $t$  是  $k$  上一个超越元.  $K = k(t)$ ,  $F = (t^p - t)$ . 证明,  $K/F$  是一个 Galois 扩张, 且  $G(K/F) \cong \mathbb{Z}/(p)$  (以  $p$  为模的剩余类加群).

4. 设  $K_\lambda (\lambda \in \Lambda)$  都是域  $F$  的 Galois 扩域. 令  $K = \bigcap_{\lambda} K_\lambda$ . 证明  $K$  也是  $F$  的 Galois 的扩域.

5. 证明, 实数域  $\mathbb{R}$  只有唯一的自同构——恒等自同构.

[提示: 设  $\sigma \in \text{Aut } \mathbb{R}$ . 则  $\sigma|_{\mathbb{Q}} = 1$ . 再证对于任意  $a \in \mathbb{R}$ ,  $a > 0 \iff \sigma(a) > 0$ .]

6. 设  $K = \mathbb{C}(x, y)$  是复数域  $\mathbb{C}$  上不定元  $x$  和  $y$  的有理分式域,  $F = \mathbb{C}(x^n + y^n, xy)$ . 证明  $K/F$  是 Galois 扩张, 它的 Galois 群  $G(K/F)$  是由  $\sigma: (x, y) \mapsto (y, x)$  和  $\tau: (x, y) \mapsto (\zeta x, \zeta^{-1}y)$  ( $\zeta = e^{2\pi i/n}$ ) 所生成的  $2n$  阶群 (二面体群).

7. 设  $K$  是域  $F$  上一个有限次 Galois 扩域,  $E$  是  $K/F$  的一个中间域. 证明, 存在  $E$  的唯一的极小扩域  $L$ ,  $F \subseteq E \subseteq L \subseteq K$ . 使得  $L/F$  是 Galois 扩张, 并且

$$G(K/L) = \bigcap_{\sigma \in G(K/F)} \sigma G(K/E) \sigma^{-1}.$$

8. 设  $K$  是域  $F$  上一个有限次 Galois 扩域.  $L, M$  是  $K/F$  的中间域. 证明

$$(i) \quad G(K/LM) = G(K/L) \cap G(K/M);$$

$$(ii) \quad G(K/L \cap M) = G(K/L) \vee G(K/M),$$

这里  $G(K/L) \vee G(K/M)$  表示  $G(K/L)$  与  $G(K/M)$  所生成的子群, 即  $G(K/F)$  中包含  $G(K/L)$  及  $G(K/M)$  的最小的子群;

(iii) 如果  $G(K/L) \cap G(K/M) = \{1\}$ , 可以得出什么结论?

9. 设  $L$  是域  $F$  的一个正规扩域,  $K$  是  $F$  在  $L$  中的可分闭包. 证明  $K$  是  $F$  的 Galois 扩域.

10. 设  $F$  是一个完备域,  $\Omega$  是  $F$  的一个代数闭包. 证明  $\Omega$  是  $F$  的 Galois 扩域.

### 3.2 一些例子

在叙述 Galois 理论的基本定理之前, 我们先看几个例子.

例 1 令  $F$  是一个特征不等于 2 的域,  $K$  是  $F$  的一个二次扩域. 则  $K$  是  $F$  的 Galois 扩域.

事实上. 设  $\alpha \in K$  但  $\alpha \notin F$ , 那么  $K = F(\alpha)$ .  $\alpha$  在  $F$  上的最小多项式是  $f(X) = X^2 + bX + c$ . 因为  $\text{char } F \neq 2$ , 所以  $f'(X) = 2X + b \neq 0$ ,  $f(X)$  是可分的, 从而  $K = F(\alpha)$  是  $F$  上可分扩域. 令  $m = b^2 - 4c$ , 则  $K = F(\sqrt{m}) = F(\sqrt{m}, -\sqrt{m})$ , 所以  $K$  是多项式  $X^2 - m$  在  $F$  上的分裂域, 因而是  $F$  上 Galois 扩域.

例 2 令  $K$  是域  $F$  的正规扩域;  $K_s$  是  $F$  在  $K$  中的可分闭包. 则  $K_s$  是  $F$  的 Galois 扩域.

事实上,  $K_s/F$  是可分的. 我们只需证明  $K_s/F$  是正规的. 设  $\alpha \in K_s$ . 令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式. 由 2.3.2, 在  $K[X]$  内,  $f(X)$  可以分解成一次因式的乘积:

$$f(X) = \prod_{i=1}^n (X - \alpha_i), \alpha_i \in K (1 \leq i \leq n).$$

因为  $\alpha$  是  $F$  上可分元素, 而  $f(\alpha_i) = 0$ , 所以  $\alpha_i \in K_s, 1 \leq i \leq n$ . 这样,  $f(X)$  在  $K_s[X]$  内可以分解成一次因式的积. 再由 2.3.2,  $K_s$  是  $F$  的正规扩域.

例3 设  $F$  是一个完备域;  $\Omega$  是  $F$  的代数闭包. 则  $\Omega$  是  $F$  的可分正规扩域, 从而是 Galois 扩域. 特别当  $\text{Char } F = 0$  或者  $F$  是有限域时,  $\Omega$  是  $F$  的 Galois 扩域.

例4 令  $\mathbb{Q}$  是有理数域. 多项式  $X^3 - 2$  在  $\mathbb{Q}[X]$  中不可约,  $E = \mathbb{Q}(\sqrt[3]{2})$  是  $\mathbb{Q}$  的一个三次扩域. 在复数域  $\mathbb{C}$  上,  $X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta\sqrt[3]{2})(X - \zeta^2\sqrt[3]{2})$ ,  $\zeta = e^{2\pi i/3}$ . 因此  $K = \mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$  是  $X^3 - 2$  在  $\mathbb{Q}$  上的分裂域, 因而是  $\mathbb{Q}$  上一个 Galois 扩域.  $[K : \mathbb{Q}] = 6$ .  $[K : E] = 2$ , 所以由例1,  $K/E$  是 Galois 扩张. 然而  $E = \mathbb{Q}(\sqrt[3]{2}) \ni \zeta\sqrt[3]{2}$  ( $\sqrt[3]{2}$  的共轭元素), 所以  $E/\mathbb{Q}$  不是 Galois 扩张.

我们确定 Galois 群  $G = G(K/\mathbb{Q})$ .  $G$  的任意元素  $\sigma$  由  $K$  在  $\mathbb{Q}$  上的生成元  $\sqrt[3]{2}$  和  $\zeta$  的像  $\sigma(\sqrt[3]{2})$  和  $\sigma(\zeta)$  完全确定.  $\sigma(\sqrt[3]{2})$  和  $\sigma(\zeta)$  可能的值是它们在  $\mathbb{Q}$  上的共轭元,  $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2} = \zeta^{-1}\sqrt[3]{2}$  和  $\zeta, \zeta^{-1} = \zeta^2$ . 这样的共轭元素对  $(\sigma(\sqrt[3]{2}), \sigma(\zeta))$  共有六种可能. 另一方面, 由 3.1.4,  $|G| = [K : \mathbb{Q}] = 6$ . 因此上述六个共轭元素对完全确定了群  $G$  的元素.

令  $\sigma, \tau \in G$ , 它们分别是由元素对  $(\sigma\sqrt[3]{2}, \sigma(\zeta)) = (\zeta\sqrt[3]{2}, \zeta)$  和  $(\tau(\sqrt[3]{2}), (\tau(\zeta)) = (\sqrt[3]{2}, \zeta^{-1})$  所决定  $K$  的  $\mathbb{Q}$ -自同构, 那么

$$G = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \tau^2\tau\}.$$

$G$  的元素由以下的表给出 ( $\rho$  代表  $G$  的一般元素):

$\rho$	$\rho(\sqrt[3]{2})$	$\rho(\zeta)$	阶
1	$\sqrt[3]{2}$	$\zeta$	1
$\sigma$	$\zeta\sqrt[3]{2}$	$\zeta$	3
$\sigma^2$	$\zeta^{-1}\sqrt[3]{2}$	$\zeta$	3
$\tau$	$\sqrt[3]{2}$	$\zeta^{-1}$	2
$\sigma\tau$	$\zeta\sqrt[3]{2}$	$\zeta^{-1}$	2
$\sigma^2\tau$	$\zeta^{-1}\sqrt[3]{2}$	$\zeta^{-1}$	2

$G \cong S_3$ .

**例 5** 令  $p$  是一个素数.  $X^4 - p$  是  $\mathbb{Q}[X]$  中不可约多项式. 令  $\alpha = \sqrt[4]{p} \in R$ .  $E = \mathbb{Q}(\alpha)$  是  $\mathbb{Q}$  上四次扩域.  $K = E(i) = \mathbb{Q}(\alpha, i)$  是  $X^4 - p$  在  $\mathbb{Q}$  上的分裂域. 因而  $K$  是  $\mathbb{Q}$  上一个 Galois 扩域.  $[K : \mathbb{Q}] = 8$ ,  $\mathbb{Q} \subsetneq E \subsetneq K$ .  $E \ni i\alpha$  ( $\alpha$  的  $\mathbb{Q}$ -共轭元), 所以  $E/\mathbb{Q}$  不是 Galois 扩张.

令  $G = G(K/\mathbb{Q})$ .  $G$  的任意元素  $\rho$  由它在  $\alpha$  和  $i$  上的作用完全确定.  $\rho(\alpha)$  可能取的值是  $\pm\alpha, \pm i\alpha$ ;  $\rho(i)$  可能取的值是  $\pm i$ , 所以元素对  $(\rho(\alpha), \rho(i))$  共有 8 种可能. 然而由 3.1.4,  $|G| = 8$ . 所以这样的八对元素恰好确定了  $G$  的全部元素. 取  $\sigma, \tau \in G$ , 分别是由元素对  $(\sigma(\alpha), \sigma(i)), = (i\alpha, i)$  和  $(\tau(\alpha), (\tau(i)) = (\alpha, -i)$  所确定的元素. 则

$$G = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

$G$  与二面体群  $D_4$  同构,  $G$  的元素由下面的表给出:

$\rho$	$\rho(\alpha)$	$\rho(i)$	阶
1	$\alpha$	$i$	1
$\sigma$	$i\alpha$	$i$	4
$\sigma^2$	$-\alpha$	$i$	2
$\sigma^3$	$-i\alpha$	$i$	4
$\tau$	$\alpha$	$-i$	2
$\sigma\tau$	$i\alpha$	$-i$	2
$\sigma^2\tau$	$-\alpha$	$-i$	2
$\sigma^3\tau$	$-i\alpha$	$-i$	2

**例 6** 有限域的 Galois 群.

设  $F = F_q$  是  $q$  元有限域,  $K$  是  $F$  的一个  $f$  次扩域.  $K = Fq^f$  是可分多项式  $X^{q^f} - X \in F[X]$  在  $F$  上的分裂域, 因而是  $F$  的 Galois 扩域.

$K$  的乘法群  $K^\times = K \setminus \{0\}$  是一个  $q^f - 1$  阶循环群, 它由一个元素  $\theta \in K^\times$  生成.

$$\sigma : K \ni \alpha \mapsto \alpha^q \in K$$

是  $K$  的一个  $F$ -自同构, 所以  $\sigma \in G(K/F)$ .

设  $\sigma$  的阶为  $m$ . 那么

$\sigma^m = 1 \iff \sigma^m(\alpha) = \alpha, \forall \alpha \in K \iff \theta = \sigma^m(\theta) = \theta^{q^m} \iff \theta^{q^m - 1} = 1$ . 因为  $\theta$  的阶是  $q^f - 1$ , 而  $m$  是使  $\sigma^m = 1$  的最小正整数, 所以  $m = f$ . 这样,  $1, \sigma, \dots, \sigma^{f-1}$  是  $G(K/F)$  中互不相同的元素. 然而由 3.1.4,  $|G(K/F)| = [K : F] = f$ . 所以

$$G(K/F) = \{1, \sigma, \dots, \sigma^{f-1}\}$$

是由  $\sigma$  所生成的  $f$  阶循环群.

## 习 题

1. 设  $\text{char } F \neq 3$ ,  $K$  是域  $F$  上一个三次不可约多项式的一个分裂域. 证明  $G(K/F)$  同构于三次对称群或三次交错群.

2. 设  $K = \mathbb{Q}(\sqrt{2}, i)$ . 试求  $K/\mathbb{Q}$  的 Galois 群及群表.

3. 设  $F$  是一个域,  $K = F(\alpha)$ ,  $\alpha^n = 1$ , 其中  $n$  是使得等式  $\alpha^n = 1$  成立的最小正整数. 证明,  $K/F$  的 Galois 群是 Abel 群.

4. (i) 设  $d \in \mathbb{Q}$ , 且  $d \geq 0$ ,  $K = \mathbb{Q}(\sqrt{d})$ , 证明  $G(K/\mathbb{Q})$  或者是单位元群或者同构于  $\mathbb{Z}/2\mathbb{Z}$ .

(ii) 证明复数域  $\mathbb{C}$  是实数域  $\mathbb{R}$  上的 Galois 扩域.

5. 设  $F(X)$  是域  $F$  上不定元  $X$  的有理分式域,  $G = \{1, \sigma, \tau\} \subset G(F(X)/F)$ , 其中  $1$  是恒等自同构,  $\sigma$  和  $\tau$  分别是由

$$X \mapsto \frac{1}{1-X} \text{ 和 } X \mapsto \frac{X-1}{X}$$

所导出的  $F(X)$  的  $F$ -自同构. 证明,  $G$  是  $G(F(X)/F)$  的子群, 并且确定  $G$  的固定域  $F(X)^G$ .



### 3.3 基本定理

在这一节里，我们将叙述并且证明 Galois 理论的基本定理。

设  $K/F$  是一个 Galois 扩张,  $G = G(K/F)$  是它的 Galois 群. 由 3.1.1, 我们有

$$F = K^G = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}.$$

设  $H$  是  $G$  的一个子群. 那么显然有

$$F = K^G \subseteq K^H \subseteq K.$$

即  $H$  的固定域  $K^H$  是  $K/F$  的一个中间域. 反过来设  $E$  是  $K/F$  的一个中间域. 由 3.1.6,  $K/E$  也是 Galois 扩张, 并且  $G(K/E)$  是  $G$  的一个子群.

令  $\{H\}$  是  $G$  的子群族 ( $G$  的一切子群所组成的集),  $\{E\}$  是  $K/F$  的中间域族. 那么

$$\Phi: H \mapsto K^H$$

定义了  $\{H\}$  到  $\{E\}$  的一个映射, 另一方面.

$$\Gamma: E \mapsto G(K/E)$$

是  $\{E\}$  到  $\{H\}$  的一个映射. 我们考虑合成映射  $\Phi \circ \Gamma$  和  $\Gamma \circ \Phi$ . 因为  $K/E$  是 Galois 扩张, 所以

$$\Phi \circ \Gamma(E) = \Phi(G(K/E)) = K^{G(K/E)} = E.$$

即  $\Phi \circ \Gamma$  是  $\{E\}$  到自身的恒等映射. 另一方面, 映射  $\Gamma \circ \Phi$  不一定是  $\{H\}$  到自身的恒等映射 (参看本节习题7). 然而这种情况只有在  $K$  是  $F$  的无限次扩域时才有可能发生. 我们将证明, 当  $K$  是  $F$  的有限次扩域时,  $\Gamma \circ \Phi$  也是恒等映射, 从而在  $\{H\}$  与  $\{E\}$  之间可以建立一个双射.

先证以下的

**引理 3.3.1** 设  $K$  是一个域,  $G$  是  $K$  的全体自同构群  $\text{Aut}(K)$  的一个有限子群,  $F = K^G$  是  $G$  的固定域. 则

$$[K : F] \leq |G|.$$

证 设  $n = |G|$ . 我们只需证明,  $K$  中任意  $m > n$  个元素都在  $F$  上线性相关. 令  $G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$ . 设  $\alpha_1, \alpha_2, \dots, \alpha_m$  是  $K$  中  $m > n$  个元素. 那么以下的系数在  $K$  内  $m$  个未知量  $x_1, x_2, \dots, x_m$ ,  $n$  个方程的齐次线性方程组

$$(1) \quad \sum_{j=1}^m \sigma_i(\alpha_j) x_j = 0, i = 1, 2, \dots, n,$$

在  $K$  中有非零解. 在所有这样的非零解中, 选取一个解  $(b_1, b_2, \dots, b_m)$  使得所含非零分量  $b_j$  的个数最少. 必要时重新对未知量编号, 可设  $b_1 \neq 0$ . 又因为  $b_1^{-1}(b_1, b_2, \dots, b_m)$  也是方程组的一个解, 所以我们不妨假设  $b_1 = 1$ . 我们证明, 每一个  $b_j$  都在  $F$  内, 从而方程组(1)的第一个方程( $\sigma_1 = 1$ )就是

$$\alpha_1 + b_2 \alpha_2 + \dots + b_m \alpha_m = 0,$$

由此就得出  $\alpha_1, \alpha_2, \dots, \alpha_m$  在  $F$  上线性相关.

如果某一个  $b_j \notin F$ , 不失一般性可设  $b_2 \notin F$ . 由于  $F = K^G$ , 所以有  $\sigma_k \in G$ , 使得  $\sigma_k(b_2) \neq b_2$ . 把  $\sigma_k$  作用于方程组

$$\sum_{j=1}^m \sigma_i(\alpha_j) b_j = 0, 1 \leq i \leq n$$

的每一个方程, 我们得到

$$\sum_{j=1}^m \sigma_k \sigma_i(\alpha_j) \sigma_k(b_j) = 0, 1 \leq i \leq n.$$

然而  $\{\sigma_k \sigma_1, \dots, \sigma_k \sigma_n\} = \{\sigma_1, \dots, \sigma_n\}$ , 所以

$$\sum_{j=1}^m \sigma_i(\alpha_j) \sigma_k(b_j) = 0, 1 \leq i \leq n.$$

这就是说,  $(1, \sigma_k(b_2), \dots, \sigma_k(b_m))$  也是方程组(1)的一个解. 由解  $(1, b_2, \dots, b_m)$  减去这个解得  $(0, b_2 - \sigma_k(b_2), \dots, b_m - \sigma_k(b_m))$ , 它仍是(1)的非平凡解, 因为  $b_2 - \sigma_k(b_2) \neq 0$ . 这个解所含非零分量的个数小于  $(b_1, b_2, \dots, b_m)$  中非零分量的个数, 这与  $(b_1, b_2, \dots, b_m)$  的取法矛盾. 这样, 必须所有  $b_j \in F$ . ■

**定理 3.3.2** 令  $K$  是一个域,  $G$  是  $K$  的全体自同构群  $\text{Aut}(K)$  的一个子群.  $F = K^G$  是  $G$  的固定域. 如果  $G$  是有限群, 那么  $K$  是  $F$  的有限次 Galois 扩域, 并且  $G$  就是扩张  $K/F$  的 Galois 群.

**证** 如果  $|G| < \infty$ , 那么由 3.3.1,  $[K:F] \leq |G|$ , 所以  $K$  是  $F$  的有限次 Galois 扩域. 由 3.1.4, 我们有  $|G(K/F)| = [K:F]$ . 注意到  $G \subseteq G(K/F)$ , 于是  $G = G(K/F)$ . ■

现在我们来陈述和证明 Galois 理论的基本定理.

**定理 3.3.3** (Galois 理论的基本定理) 设  $K$  是域  $F$  的一个有限次 Galois 扩域.  $G = G(K/F)$  是  $K/F$  的 Galois 群. 对于  $G$  的每一个子群  $H$ , 令  $H$  的固定域  $E = K^H$  与它对应, 那么  $\Phi: H \mapsto E$  是  $G$  的子群族与  $K/F$  的中间域族之间的一个双射.

**证** 设  $E$  是  $K/F$  的一个中间域, 我们已经看到.

$$\Gamma: E \mapsto G(K/E)$$

是  $K/F$  的中间域族  $\{E\}$  到  $G$  的子族  $\{H\}$  的一个映射, 并且对于任意中间域  $E$ ,  $\Phi \circ \Gamma(E) = E$ . 只剩下证明,  $\Gamma \circ \Phi$  是  $G$  的子群族  $\{H\}$  的恒等映射.

因为  $K/F$  是有限次 Galois 扩张, 所以  $G$  是有限群, 设  $H$  是  $G$  的任意一个子群. 令  $E = \Phi(H) = K^H$  是  $H$  的固定域. 由 3.3.2,  $H = G(K/E) = \Gamma(\Phi(H))$ , 这就是说,  $\Gamma \circ \Phi$  是  $G$  的子群族  $\{H\}$  的恒等映射. 因而  $\Phi$  是双射. ■

我们以下用  $H \longleftrightarrow E$  表示子群族  $\{H\}$  与中间域族  $\{E\}$  的如上定义的双射. 关于这个双射的细节, 有以下

**定理 3.3.4** 设  $K$  是域  $F$  的一个有限次 Galois 扩域.  $G$  是  $K/F$  的 Galois 群. 在 3.3.3 中所定义的  $G$  的子群族  $\{H\}$  与  $K/F$  的中间域族  $\{E\}$  之间的双射满足以下条件:

(i)  $G \longleftrightarrow F; \{1\} \longleftrightarrow K$ .

(ii) 设  $H \longleftrightarrow E$ , 则  $[K:E] = |H|, [E:F] = (G:H)$ ,

这里  $(G : H)$  表示子群  $H$  对于  $G$  的指数.

$$(iii) \quad H_i \longleftrightarrow E_i, \quad i=1,2, \quad H_1 \subseteq H_2 \iff E_1 \supseteq E_2.$$

$$(iv) \quad H \longleftrightarrow E, \quad \sigma \in G, \quad \text{则 } \sigma H \sigma^{-1} \longleftrightarrow \sigma(E).$$

(v)  $H_i \longleftrightarrow E_i, i=1,2$ , 则  $H_1$  与  $H_2$  在  $G$  中共轭  $\iff E_1$  与  $E_2$  在  $F$  上共轭.

(vi)  $H \longleftrightarrow E$ ,  $H$  是  $G$  的正规子群  $\iff E$  是  $F$  的 Galois 扩域; 在这个情况下  $G(E/F) \cong G/H$ .

证 (i) 是显然的.

(ii) 因为  $H = G(K/E)$ , 由 3. 1. 4,  $[K : E] = |H|$ . 于是

$$[E : F] = [K : F] / [K : E] = |G| / |H| = (G : H).$$

(iii) 显然.

(iv) 令  $E' = \sigma(E)$ . 设  $\tau \in \text{Aut}(K)$ . 那么

$$\begin{aligned} \tau \in G(K/E') &\iff \tau(\beta) = \beta, \quad \forall \beta \in E' = \sigma(E) \\ &\iff \tau \sigma(\alpha) = \sigma(\alpha), \quad \forall \alpha \in E \\ &\iff \sigma^{-1} \tau \sigma(\alpha) = \alpha, \quad \forall \alpha \in E \\ &\iff \sigma^{-1} \tau \sigma \in H \\ &\iff \tau \in \sigma H \sigma^{-1}, \end{aligned}$$

所以  $G(K/E') = \sigma H \sigma^{-1}$ .

(v) 设存在  $\sigma \in G$  使得  $\sigma H_1 \sigma^{-1} = H_2$ . 由 (iv) 就有  $\sigma(E_1) = E_2$ . 反之, 设  $E_1, E_2$  在  $F$  上共轭. 因为  $K/F$  是 Galois 扩张, 所以  $E_1$  到  $E_2$  的  $F$ -共轭可以开拓为  $K$  的一个  $F$ -自同构, 即存在  $\sigma \in G = G(K/F)$  使得  $\sigma(E_1) = E_2$ . 由 (iv),  $\sigma H_1 \sigma^{-1} = H_2$ .

(iv) 设  $H$  是  $G$  的正规子群. 那么

$$\sigma H \sigma^{-1} = H, \quad \forall \sigma \in G.$$

由 (iv),

$$\sigma(E) = E, \quad \forall \sigma \in G.$$

令  $\sigma' = \sigma|_E$ . 则  $\sigma' \in G(E/F)$ . 映射

$$f: G \ni \sigma \mapsto \sigma' \in G(E/F)$$

是群  $G$  到群  $G(E/F)$  的同态映射. 设  $\sigma' \in G(E/F)$ . 因为  $K/F$  是正规扩张, 所以  $\sigma'$  可以开拓为  $G$  的一个元素  $\sigma$ , 即存在  $\sigma \in G$ , 使得  $\sigma|_E = \sigma'$ . 所以  $f$  是满同态.

$\text{Ker}(f) = \{\sigma \in G \mid \sigma(\alpha) = \alpha, \forall \alpha \in E\} = G(K/E) = H$ .  
所以  $G(E/F) \cong G/H$ .

由(ii),  $[E:F] = (G:H) = |G(E/F)|$ , 由 3.1.4,  $E/F$  是 Galois 扩张.

反之, 如果  $E/F$  是 Galois 扩张, 那么  $E/F$  是正规扩张, 所以  $\sigma(E) = E, \forall \sigma \in G$ . 由(iv),  $\sigma H \sigma^{-1} = H, \forall \sigma \in G \implies H$  是正规子群. ■

例 1  $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$  是有理数域  $\mathbb{Q}$  上 6 次 Galois 扩张.  $K/\mathbb{Q}$  的 Galois 群  $G = G(K/\mathbb{Q})$  由

$$\sigma: (\sqrt{-3}, \sqrt[3]{2}) \mapsto (\sqrt{-3}, \zeta \sqrt[3]{2})$$

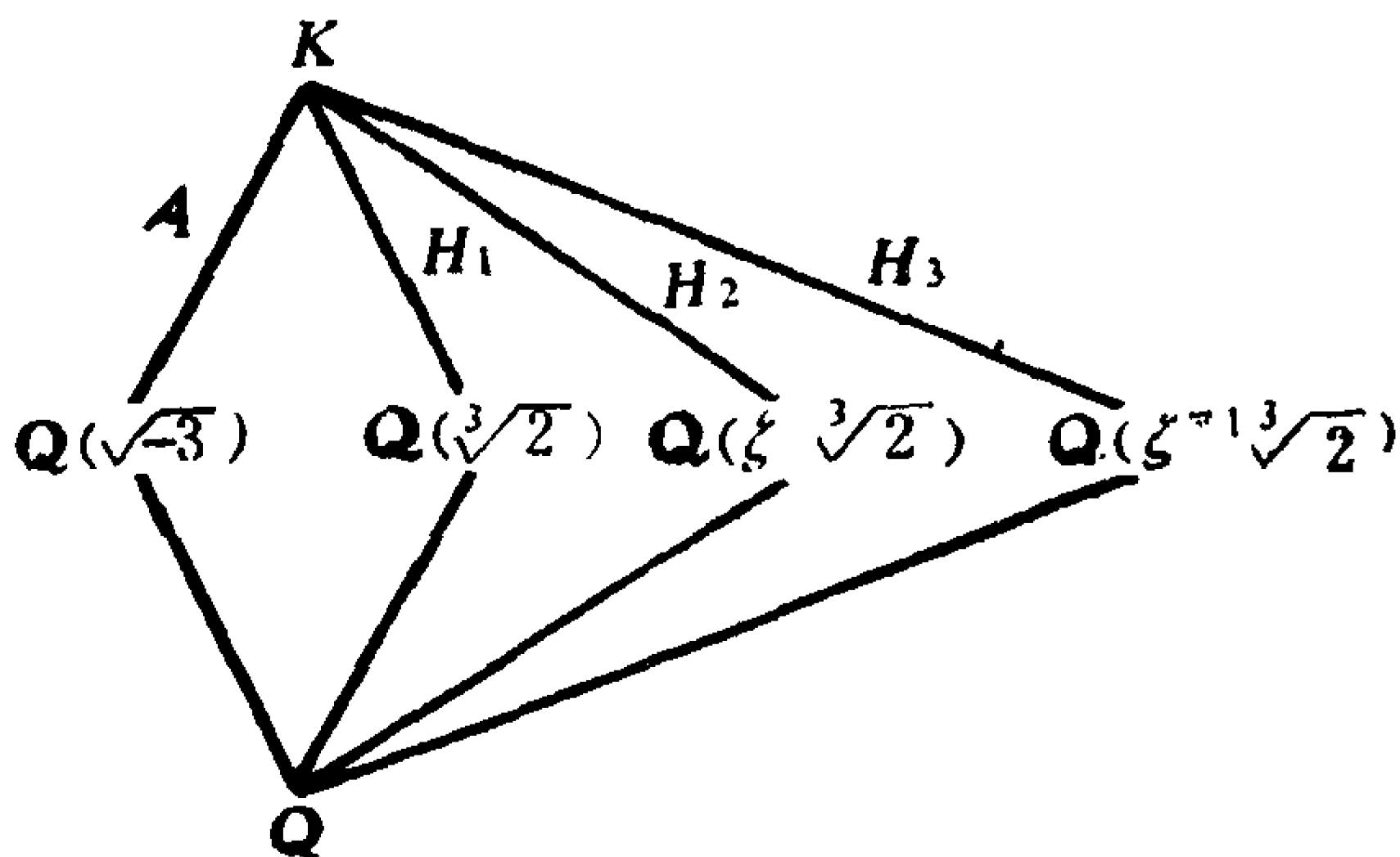
$$\tau: (\sqrt{-3}, \sqrt[3]{2}) \mapsto (-\sqrt{-3}, \sqrt[3]{2})$$

生成, 这里  $\zeta = e^{2\pi i/3}$ ,  $G \cong S_3$  (参看 § 3.2, 例 4).

$$G = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\},$$

$$\sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2$$

$G$  共有四个真子群:



$$A = \{1, \sigma, \sigma^2\}$$

$$H_1 = \{1, \tau\}, H_2 = \{1, \sigma^2 \tau\}, H_3 = \{1, \sigma \tau\}.$$

其中  $A$  是正规子群。我们有

$$\sigma H_1 \sigma^{-1} = H_2, \sigma^2 H_1 \sigma^{-2} = H_3.$$

所以  $H_1, H_2, H_3$  是两两共轭的子群。

$K/Q$  的中间域与  $G$  的子群之间的对应关系见 84 页的图。

例 2  $K = Q(\sqrt[4]{3}, i)$ ,  $i = \sqrt{-1}$ , 是有理数域  $Q$  上 8 次 Galois 扩域。  $K/Q$  的 Galois 群  $G$  是由

$$\sigma : (\sqrt[4]{3}, i) \mapsto (i\sqrt[4]{3}, i),$$

$$\tau : (\sqrt[4]{3}, i) \mapsto (\sqrt[4]{3}, -i)$$

所生成的 8 阶二面体群 (参看 3.2, 例 5)。

$$G = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

$$\sigma^4 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^3.$$

$G$  的真子群计有

五个二阶子群:

$$H_1 = \{1, \sigma^2\}; H_2 = \{1, \sigma^3\tau\}; H_3 = \{1, \sigma\tau\};$$

$$H_4 = \{1, \sigma^2\tau\}; H_5 = \{1, \tau\}.$$

三个四阶子群 (正规子群):

$$J_1 = \{1, \sigma, \sigma^2, \sigma^3\};$$

$$J_2 = \{1, \sigma^2, \tau, \sigma^2\tau\} = H_1 \times H_5 = H_1 \times H_4 = H_4 \times H_5;$$

$$J_3 = \{1, \sigma^2, \sigma^3\tau, \sigma\tau\} = H_1 \times H_2 = H_1 \times H_3 = H_2 \times H_3.$$

$H_1$  是正规子群,  $\sigma H_2 \sigma^{-1} = H_3, \sigma H_5 \sigma^{-1} = H_4.$

令  $E_i = \Phi(H_i) = K^{H_i}, i = 1, 2, 3, 4, 5$

$$L_i = \Phi(J_i) = K^{J_i}, i = 1, 2, 3.$$

则

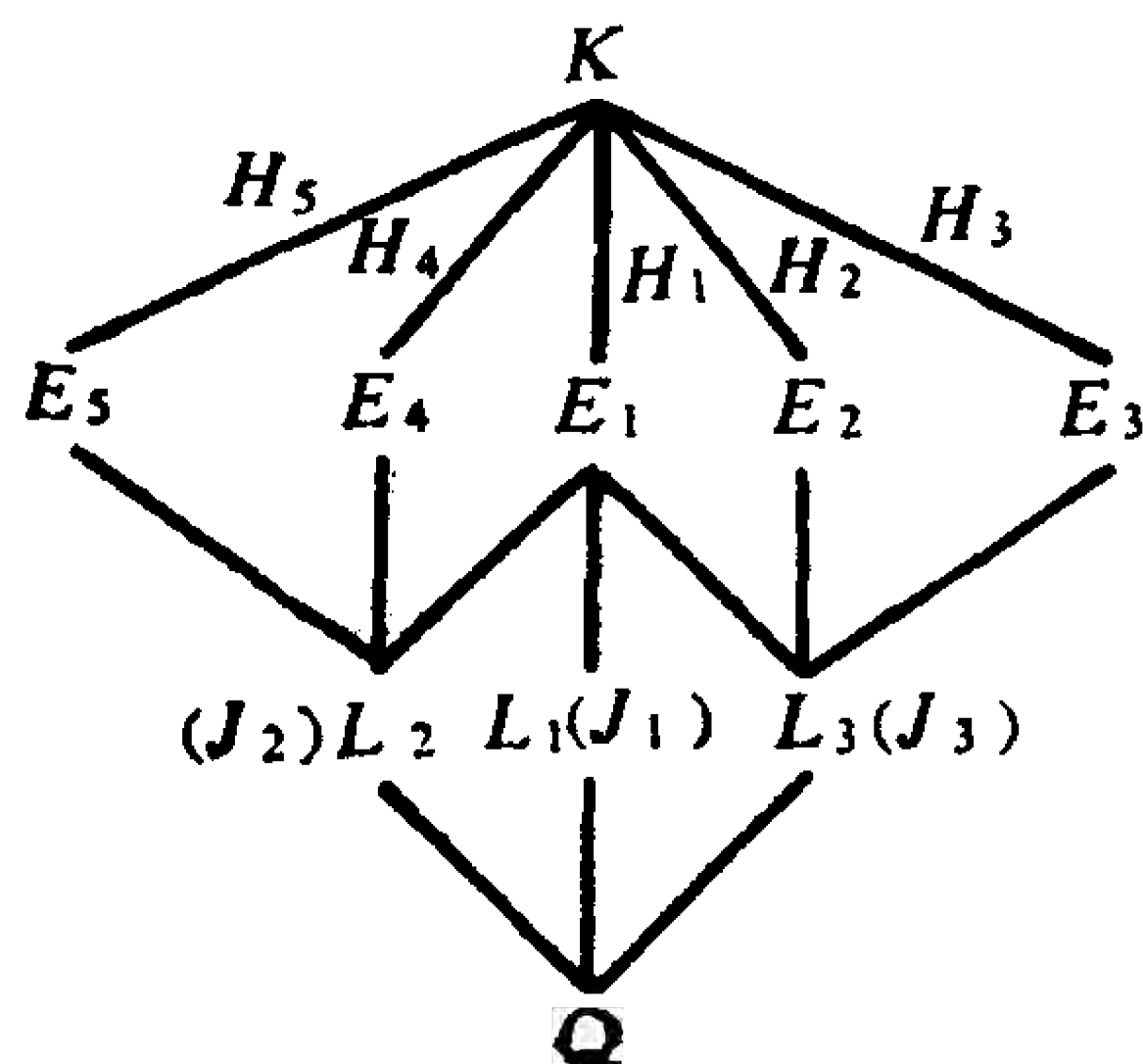
$$E_1 = Q(\sqrt[4]{3}, i), E_2 = Q((1-i)\sqrt[4]{3}),$$

$$E_3 = Q((1+i)\sqrt[4]{3}),$$

$$E_4 = Q(i\sqrt[4]{3}), E_5 = Q(\sqrt[4]{3}).$$

$$L_1 = \mathbb{Q}(i), L_2 = \mathbb{Q}(\sqrt{3}), L_3 = \mathbb{Q}(i\sqrt{3}).$$

它们的关系由下图表示:



## 习 题

1. 设  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . 则  $K/\mathbb{Q}$  是 Galois 扩张 (3.1, 习题 1). 写出 Galois 群  $G(K/\mathbb{Q})$  的子群与  $K/\mathbb{Q}$  的中间域之间的对应关系.

2. 设  $K/F$  是一个有限次 Galois 扩张,  $G = G(K/F)$  是它的 Galois 群, 且  $G$  可以写成它的子群  $H_1$  与  $H_2$  的直积:  $G = H_1 \times H_2$ . 令  $K_i = K^{H_i}$ ,  $i = 1, 2$ , 证明,  $K = K_1 K_2$ .

3. 设  $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt{5})$ .

(i) 证明  $K/\mathbb{Q}$  是 Galois 扩张.

(ii) 决定 Galois 群  $G(K/\mathbb{Q})$ .

(iii) 求出  $G(K/\mathbb{Q})$  的所有子群及  $K/\mathbb{Q}$  的所有中间域.

4. 设  $K_1$  和  $K_2$  都是域  $F$  的有限次 Galois 扩域, 并且都包含在  $F$  的某一个扩域内.

(i) 证明,  $K_1 K_2$  是  $F$  的 Galois 扩域.

(ii) 令

$H = \{(\sigma_1, \sigma_2) \mid \sigma_i \in G(K_i/F), i=1, 2, \text{ 且 } \sigma_1|_{K_1 \cap K_2} = \sigma_2|_{K_1 \cap K_2}\}$ . 证明,  $H$  是直积  $G(K_1/F) \times G(K_2/F)$  的子群, 且

$$G(K_1 K_2/F) \cong H.$$

(iii) 如果  $K_1 \cap K_2 = F$ , 则

$$G(K_1 K_2/F) \cong G(K_1/F) \times G(K_2/F).$$

5. 设  $f(X)$  是域  $F$  上一个多项式,  $K$  是  $f(X)$  在  $F$  上一个分裂域. 在  $K[X]$  内,

$$f(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_s)^{k_s}.$$

$\alpha_i \in K$ , 且互不相同,  $k_i > 0$  ( $1 \leq i \leq s$ ). 令

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_s)$$

又令  $u_0, u_1, \dots, u_s \in K$  是  $g(X)$  的系数,  $E = F(u_0, u_1, \dots, u_s)$ . 证明  $K/E$  是 Galois 扩张, 且  $G(K/E) \cong G(K/F)$ .

6. 设  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ,

$$\alpha = \sqrt{\sqrt{6}(\sqrt{2} + \sqrt{3})(1 + \sqrt{2})}, \quad K = E(\alpha).$$

(i) 证明,  $E/\mathbb{Q}$  是四次 Galois 扩张, 且  $G(E/\mathbb{Q})$  与 Klein 四元群同构.

(ii) 设  $G(E/\mathbb{Q}) = \{1_E, \sigma, \tau, \rho\}$ . 算出  $\rho(\alpha^2)$ ,  $\sigma(\alpha^2)$  和  $\tau(\alpha^2)$ .

(iii) 设  $\varepsilon, \tilde{\rho}, \sigma, \tau$  是  $K$  的  $\mathbb{Q}$ -共轭, 满足条件:  $\varepsilon|_E = 1_E$ ,  $\sigma|_E = \sigma$ ,  $\tau|_E = \tau$ ,  $\tilde{\rho}|_E = \rho$ . 计算  $\varepsilon(\alpha)$ ,  $\tilde{\rho}(\alpha)$ ,  $\sigma(\alpha)$  和  $\tau(\alpha)$ .

(iv) 证明  $\alpha \in E$ , 从而  $K/\mathbb{Q}$  是八次 Galois 扩张.

(v) 证明,  $G(K/\mathbb{Q})$  由  $\sigma$  和  $\tau$  生成, 并且满足关系

$$\sigma^4 = 1, \tau^{-1} \sigma \tau = \sigma^{-1}, \tau^2 = \sigma^2.$$

从而  $G(K/\mathbb{Q})$  与四元数群  $Q_8$  同构.

(vi) 找出  $G(K/\mathbb{Q})$  的一切子群与  $K/\mathbb{Q}$  的一切中间域之间的对应关系.

7. 令  $F = F_p$  是一个  $p$  元有限域,  $p$  是一个素数,  $\Omega$  是  $F$  的



一个代数闭包。则，取定一个整数  $l > 2$ 。令  $F_i$  表示  $F$  上  $\Omega$  中唯一的  $l^i$  次扩域  $F_{q_i}$ ,  $q_i = p^i$ 。

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset \Omega.$$

$$\text{令 } N = \bigcup_{i \geq 0} F_i.$$

(i) 证明,  $N$  是  $F$  的 Galois 扩域。

(ii) 令  $\varphi: N \ni \alpha \mapsto \alpha^p \in N$ 。证明  $\varphi$  是  $N$  的一个  $F$ -自同构, 从而  $\varphi$  属于  $N/F$  的 Galois 群  $G(N/F)$ 。

(iii) 令  $G = G(N/F)$ 。设

$$H = \{\varphi^n \mid n \in \mathbb{Z}\}$$

是  $G$  中由  $\varphi$  所生成的循环子群。证明:

(a)  $\Phi(H) = \Phi(G) = F$ ;

(b)  $G \neq H$ 。

从而对于 Galois 扩张  $N/F$  来说,  $\Gamma \circ \Phi$  不是  $G$  的子群族的恒等映射。

[提示] 要证明 (b) 成立, 可令

$$l_i = 1 + l + \cdots + l^{i-1} = (1 - l^i)/(1 - l), i \geq 1.$$

对于任意  $\alpha \in N$ , 则  $\alpha \in F_i$ , 对于某个  $i$ 。定义  $\sigma(\alpha) = \varphi^{l_i}(\alpha)$ 。证明  $\sigma$  的定义不依赖于  $i$ , 因而  $\sigma(\alpha)$  是由  $\alpha$  唯一确定的, 并且  $\sigma \in G$ , 但  $\sigma \notin H$ 。

### 3.4 单位根

为了以下的讨论, 在这一节里, 先作一些准备工作。

设  $F$  是一个域。  $F^\times$  是  $F$  的一切非零元素所构成的乘法群。

$n$  是一个正整数。  $\zeta \in F$  叫做一个  $n$  次单位根, 如果  $\zeta^n = 1$ 。

$F$  中一个  $n$  次单位根  $\zeta$  叫做一个本原  $n$  次单位根, 如果对于任意小于  $n$  的正整数  $m$  来说,  $\zeta^m \neq 1$ 。

设  $\zeta \in F$ 。如果  $\zeta$  是某一个  $n$  次单位根, 那么就称  $\zeta$  是一个

单位根.

令  $W_F$  表示  $F$  中一切单位根的集. 则  $W_F$  是  $F^\times$  的一个子群.  
令  $W_n$  表示  $F$  中一切  $n$  次单位根所成的集. 则  $W_n$  是  $W_F$  的一个有限子群.

**定理 3.4.1** (i)  $W_n$  是有限循环群;  $W_n$  的阶  $|W_n|$  整除  $n$ .

(ii)  $|W_n| = n \iff F$  含有本原  $n$  次单位根.

在这个情况下,  $F$  所含本原  $n$  次单位根的个数等于  $\varphi(n)$ , 这里  $\varphi(n)$  表示 Euler 函数, 即小于  $n$  且与  $n$  互素的正整数的个数.

(iii) 设  $F$  含有本原  $n_i$  次单位根,  $1 \leq i \leq s$ , 令  $n$  是  $n_1, \dots, n_s$  的最小公倍. 则  $F$  含有本原  $n$  次单位根.

(iv) 设  $\text{char } F = p > 0$ . 如果  $F$  含有本原  $n$  次单位根, 则  $p \nmid n$ .

(v) 设  $F$  是一个代数闭域. 如果  $\text{char } F = 0$ , 则对于任意  $n$ ,  $F$  含有本原  $n$  次单位根; 如果  $\text{char } F = p > 0$ , 则对于任意不被  $p$  整除的  $n$ ,  $F$  含有本原  $n$  次单位根.

**证** (i)  $W_n$  是  $F^\times$  的有限子群, 而  $F^\times$  的有限子群是循环群 (2.4.8), 所以  $W_n$  是循环群. 令  $\zeta$  是  $W_n$  的一个生成元,  $m$  是  $\zeta$  的阶. 则  $m = |W_n|$ . 因为  $\zeta^n = 1$ , 所以  $m \mid n$ , 即  $|W_n| \mid n$ .

(ii)  $|W_n| = n \iff W_n$  的生成元  $\zeta$  的阶为  $n \iff \zeta$  是  $F$  中一个本原  $n$  次单位根.

再者,  $\zeta \in F$  是一个本原  $n$  次单位根  $\iff \zeta$  是  $W_n$  的生成元. 因此,  $F$  所含的本原  $n$  次单位根的个数等于  $W_n$  的生成元的个数, 而后者显然等于  $\varphi(n)$ .

(iii) 设  $\zeta_i \in F$  是一个本原的  $n_i$  次单位根  $1 \leq i \leq s$ .  $n$  是  $n_1, \dots, n_s$  的最小公倍. 则  $\zeta_i^n = 1$ , 从而  $\zeta_i \in W_n$ . 所以  $\zeta_i$  的阶  $n_i$  整除  $|W_n|$ ,  $1 \leq i \leq s$ . 因此  $n \mid |W_n|$ . 另一方面, 由 (i),  $|W_n| \mid n$ .

这样一来就有  $|W_n| = n$ . 再由(ii),  $F$  含有一个本原  $n$  次单位根.

(iv) 设  $\zeta \in F$  是一个本原  $n$  次单位根. 如果  $p|n$ . 则  $(\zeta^{n/p})^p = 1 \implies (\zeta^{n/p} - 1)^p = 0 \implies \zeta^{n/p} = 1$ . 而  $n/p < n$ . 这与  $\zeta$  是本原  $n$  次单位根的假设相违.

(v) 设  $f(X) = X^n - 1 \in F[X]$ .  $f'(X) = nX^{n-1}$ . 在  $\text{char} F = 0$  或  $\text{char} F = p > 0$ , 而  $p \nmid n$  的情况下,  $f'(X) \neq 0$ . 所以  $f(X)$  与  $f'(X)$  互素, 因而  $f(X)$  没有重根. 因为  $F$  是代数闭域, 所以  $f(X)$  在  $F$  中有  $n$  个互不相同的根, 从而  $|W_n| = n$ . 所以  $F$  含有本原  $n$  次单位根. ■

现在我们定义分圆多项式的概念.

设  $\Omega$  是一个代数闭域. 如果  $\text{char} \Omega = 0$ , 我们取  $n$  是任意正整数; 如果  $\text{char} \Omega = p > 0$ , 我们就取  $n$  是任意一个不能被  $p$  整除的正整数. 由上面的定理可知  $\Omega$  含有  $\varphi(n)$  个本原  $n$  次单位根. 令  $P_n$  是  $\Omega$  中一切本原  $n$  次单位根所成的集.  $\Omega[X]$  的多项式

$$\Phi_n(X) = \prod_{\eta \in P_n} (X - \eta)$$

叫做一个分圆多项式.

显然,  $\deg \Phi_n(X) = \varphi(n)$ . 取定一个本原  $n$  次单位根  $\eta$ . 那么

$$\Phi_n(X) = \prod_{\substack{a=1 \\ (a,n)=1}}^{a \leq n} (X - \eta^a).$$

令  $W_n = \{\zeta \in \Omega \mid \zeta^n = 1\}$  是一切  $n$  次单位根所成的集. 由 3.4.1(ii),  $W_n$  是一个  $n$  阶循环群. 设  $\zeta \in W_n$ . 那么

$$\begin{aligned} \zeta \text{ 是一个 } d \text{ 阶元素 } (d|n) &\iff \zeta \text{ 是一个本原 } d \text{ 次单位根} \\ &\iff \zeta \text{ 是 } \Phi_d(X) \text{ 的根.} \end{aligned}$$

因此我们有

$$(1) \quad X^n - 1 = \prod_{\substack{d|n \\ 1 \leq d \leq n}} \Phi_d(X).$$

定理 3.4.2 设  $\Omega$  是一个代数闭域.

(i) 如果  $\text{char } \Omega = 0$ , 则  $\Phi_n(X)$  是一个最高次项系数是 1 的  $\varphi(n)$  次整系数多项式:  $\Phi_n(X) \in \mathbb{Z}[X]$ .

(ii) 如果  $\text{char } \Omega = p > 0$ , 则  $\Phi_n(X)$  是  $F_p$  上一个最高次项系数是 1 的  $\varphi(n)$  次多项式:  $\Phi_n(X) \in F_p[X]$ .

证 对  $n$  作归纳法.

设  $\text{char } F = 0$ . 当  $n=1$  时,  $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$  且最高次项系数是 1.

设  $n > 1$ , 我们有

$$X^n - 1 = \Phi_n(X) \prod_{\substack{d|n \\ 1 \leq d < n}} \Phi_d(X).$$

由归纳法假设,  $\prod_{\substack{d|n \\ 1 \leq d < n}} \Phi_d(X)$  是最高次项系数为 1 的整系数多项式,

因而是本原多项式, 于是由本原多项式的性质,

$$\Phi_n(X) \in \mathbb{Z}[X].$$

对于  $\text{char } \Omega = p > 0$  的情形, 同样可以对  $n$  用归纳法来证明.

现在设  $\Omega = \mathbb{C}$  是复数域. 则  $\Phi_n(X) \in \mathbb{Z}[X]$ . 在  $\mathbb{C}$  中, 全体  $n$  次单位根是

$$W_n = \{e^{2k\pi i/n} | k=0, 1, \dots, n-1\}.$$

当且仅当  $(k, n) = 1$  时,  $e^{2k\pi i/n}$  是本原  $n$  次单位根. 所以在  $\mathbb{C}[X]$  里, 分圆多项式是

$$\Phi_n(X) = \prod_{\substack{1 \leq a \leq n \\ (a, n) = 1}} (X - e^{2a\pi i/n})$$

定理 3.4.3 分圆多项式  $\Phi_n(X)$  在  $\mathbb{Q}[X]$  中不可约.

证 因为  $\Phi_n(X) \in \mathbb{Z}[X]$ , 所以只要证明,  $\Phi_n(X)$  不能分解成两个次数都低于  $\varphi(n)$  的整系数多项式的乘积. 假设  $f(X) \in \mathbb{Z}[X]$  是  $\Phi_n(X)$  的一个不可约因式. 不妨设  $f(X)$  的最高次项系

数是1.由(1),存在  $g(X) \in \mathbb{Z}[X]$  使得  $X^n - 1 = f(X)g(X)$ .  
我们证明,  $f(X)$  满足以下条件:

(\*) 设  $p$  是一个素数且  $p \mid n$ . 如果  $f(\zeta) = 0$ , 则  $f(\zeta^p) = 0$ .

事实上, 设  $f(\zeta^p) \neq 0$ . 因为在  $\mathbb{Z}[X]$  里,

$$X^n - 1 = f(X)g(X).$$

而  $\zeta^n - 1 = f(\zeta)g(\zeta) = 0$ , 所以

$$f(\zeta^p)g(\zeta^p) = (\zeta^p)^n - 1 = 0,$$

从而  $g(\zeta^p) = 0$ . 以所  $\zeta$  是多项式  $g(X^p) \in \mathbb{Z}[X]$  的根. 另一方面,  $f(X)$  也是  $\mathbb{Q}[X]$  中最高次项系数是1的不可约多项式, 所以  $f(X)$  是  $\zeta$  在  $\mathbb{Q}$  上的最小多项式. 因此, 在  $\mathbb{Q}[X]$  里,  $f(X) \mid g(X^p)$ , 从而在  $\mathbb{Z}[X]$  里,  $f(X) \mid g(X^p)$ . 于是存在  $h(X) \in \mathbb{Z}[X]$ , 使得

$$g(X^p) = f(X)h(X)$$

然而自然同态

$$\mathbb{Z} \ni u \mapsto \bar{u} \in \mathbb{Z}/(p) = F_p$$

可以开拓为多项式环的同态

$$\begin{aligned} \mathbb{Z}[X] \ni f(X) = \sum a_i X^i &\mapsto \bar{f}(X) \\ &= \sum \bar{a}_i X^i \in F_p[X]. \end{aligned}$$

因为在  $\mathbb{Z}[X]$  里,

$$X^n - 1 = f(X)g(X), \quad g(X^p) = f(X)h(X),$$

所以在  $F_p[X]$  里,

$$X^n - 1 = \bar{f}(X)\bar{g}(X), \quad \bar{g}(X^p) = \bar{f}(X)\bar{f}(X).$$

$\bar{f}(X) \in F_p[X]$ , 且  $\deg(\bar{f}(X)) = \deg(f(X)) > 0$ . 设  $\bar{u}(X)$  是  $\bar{f}(X)$  在  $F_p[X]$  内一个不可约因式. 因为在  $F_p[X]$  内,

$$\bar{g}(X^p) = \bar{g}(X)^p,$$

而  $\bar{f}(X) \mid \bar{f}(X)^p$ , 所以,  $\bar{u}(X) \mid \bar{g}(X)^p$ . 又因为  $\bar{u}(X)$  不可约, 所以  $\bar{u}(X) \mid \bar{g}(X)$ . 注意到  $X^n - 1 = \bar{f}(X)\bar{g}(X)$ , 所以  $\bar{u}(X)^2 \mid (X^n - 1)$ , 从而  $X^n - 1$  有重根. 所以  $(X^n - 1)' = nX^{n-1} = 0$ . 这样, 必须  $p \mid n$ . 这就导致矛盾. 因此(\*)成立.

现在设  $m$  是任意一个与  $n$  互素的正整数. 设  $m = \prod p_i$  是  $m$  的素因子分解. 那么对于每一个  $i$ ,  $p_i \nmid n$ . 设  $\zeta$  是  $f(X)$  的一个根. 因为  $f(X) \mid \Phi_n(X)$ , 所以  $\zeta$  是一个本原  $n$  次单位根. 由(\*), 我们有  $f(\zeta^{p_1}) = 0$ . 再由(\*),  $f(\zeta^{p_1 p_2}) = f((\zeta^{p_1})^{p_2}) = 0$ . 如此继续下去, 最后得  $f(\zeta^m) = 0$ . 因为  $(m, n) = 1$ , 所以  $\zeta^m$  也是一个本原  $n$  次单位根. 这样一来, 所有的本原  $n$  次单位根都是  $f(X)$  的根, 从而  $\Phi_n(X) \mid f(X)$ , 于是  $f(X) = \Phi_n(X)$ , 这就证明了  $\Phi_n(X)$  的不可约性. ■

**推论 3.4.4** 设  $\zeta \in \mathbb{C}$  是一个本原  $n$  次单位根. 那么  $\zeta$  在  $\mathbb{Q}$  上的最小多项式是分圆多项式  $\Phi_n(X)$ .  $\mathbb{Q}(\zeta)$  是多项式  $X^n - 1$  在  $\mathbb{Q}$  上的分裂域;  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ . ■

利用 Möbius 函数, 可以得到分圆多项式的一个很有用的表达式. 在这一节的最后, 我们介绍一下 Möbius 函数的概念.

设  $n$  是一个正整数. 令

$$n = p_1 p_2 \cdots p_\lambda$$

是  $n$  的素因子分解. 我们定义

$$\mu(n) = \begin{cases} 0, & \text{如果存在 } i \neq j \text{ 而 } p_i = p_j; \\ (-1)^\lambda, & \text{如果 } p_1, p_2, \dots, p_\lambda \text{ 两两不同;} \\ 1, & \text{如果 } n = 1. \end{cases}$$

$\mu$  称为 **Möbius 函数**.

**引理 3.4.5** 当  $n \geq 2$  时,

$$\sum_{\substack{d \mid n \\ 1 \leq d \leq n}} \mu(d) = 0,$$

这里  $\sum$  表示对  $n$  的一切正因子求和.

**证** 设

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

是  $n$  的素因子幂分解,  $p_1, p_2, \dots, p_r$  是互不相同的素数,  $e_i > 0$ ,  $1 \leq i \leq r$ . 我们有

$$\sum_{d|n} \mu(d) = \sum \mu(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}).$$

右端  $\sum$  表示对于满足条件  $0 \leq a_i \leq e_i (1 \leq i \leq r)$  的一切序列  $(a_1, a_2, \dots, a_r)$  求和. 去掉右端的和里等于零的那些项, 我们有

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + (\mu(p_1) + \mu(p_2) + \cdots + \mu(p_r)) + \\ &\quad + (\mu(p_1 p_2) + \cdots + \mu(p_{r-1} p_r)) + \cdots + \\ &\quad + \mu(p_1 p_2 \cdots p_r) \\ &= 1 - r + \binom{r}{2} \cdots + (-1)^r = (1-1)^r = 0. \end{aligned}$$

利用 Möbius 函数, 可以将分圆多项式写成比较便于计算的形式.

#### 定理 3.4.6

$$\Phi_n(X) = \prod_{\substack{d|n \\ 1 \leq d \leq n}} (X^d - 1)^{\mu(n/d)}.$$

证 利用(1), 在右边的积里, 以

$$X^d - 1 = \prod_{\substack{\delta|d \\ 1 \leq \delta \leq d}} \Phi_\delta(X)$$

代入得

$$\prod_{\substack{d|n \\ 1 \leq d \leq n}} (X^d - 1)^{\mu(n/d)} = \prod_{\substack{d|n \\ 1 \leq d \leq n}} \left( \prod_{\substack{\delta|d \\ 1 \leq \delta \leq d}} \Phi_\delta(X) \right)^{\mu(n/d)}$$

在右端双重积里, 固定每一个  $\delta$ ,  $\delta|d, d|n$ , 则  $n/\delta$  的每一个因子  $\delta'$  都有  $n/d$  的形状; 反之, 如果  $d|n$  且  $\delta|d$ , 那么  $n/d|n/\delta$ , 于是上式右端的双重积可以重新组合成以下形式:

$$\prod_{\substack{\delta|n \\ 1 \leq \delta \leq n}} \Phi_\delta(X)^{\sum_{\delta'|n/\delta} \mu(\delta')}$$

因为

$$\sum_{\delta'|n/\delta} \mu(\delta') = \begin{cases} 1, & \text{若 } n/\delta = 1, \\ 0, & \text{若 } n/\delta > 1. \end{cases}$$

所以

$$\prod_{\substack{d|n \\ 1 \leq d \leq n}} (X^d - 1)^{\mu(n/d)} = \Phi_n(X).$$

例 根据上面的表达式, 容易写出.

$$\Phi_1(X) = X - 1; \quad \Phi_2(X) = X + 1; \quad \Phi_3(X) = X^2 + X + 1;$$

$$\Phi_4(X) = X^2 + 1; \quad \Phi_6(X) = X^2 - X + 1; \quad \Phi_8(X) = X^4 + 1.$$

设  $p$  是一个素数, 那么对于任意正整数, 我们有

$$\begin{aligned} \Phi_{p^r}(X) &= (X^{p^r} - 1)(X^{p^{r-1}} - 1)^{-1} \\ &= X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1. \end{aligned}$$

## 习 题

1. 设  $n$  是一个奇数. 证明, 多项式  $X^n - 1$  在  $F$  上的分裂域也是  $X^{2n} - 1$  在  $F$  上的分裂域.

2. 设  $K$  是一个特征为  $p > 0$  的域. 证明,  $K$  内的一个  $p^e m$  次单位根总是一个  $m$  次单位根.

3. 证明,  $\mathbb{Q}$  的有限次扩域内只含有限个单位根.

4. 证明关于 Euler 函数  $\varphi$  的下列性质:

(i) 如果  $p$  是一个素数,  $n$  是一个正整数, 则  $\varphi(p^n) = p^n(1 - \frac{1}{p})$ ;

(ii) 如果  $(m, n) = 1$ , 则  $\varphi(mn) = \varphi(m)\varphi(n)$ ;

(iii) 如果  $n = p_1^{k_1} \cdots p_r^{k_r}$ , 其中  $p_i$  是两两不同的素数,  $k_i > 0$  ( $1 \leq i \leq r$ ), 则

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

(iv)  $\sum_{\substack{d|n \\ d \neq 0}} \varphi(d) = n$ ;

(v) 令  $d$  和  $l$  分别是  $m$  和  $n$  的最大公因数和最小公倍数, 则  $\varphi(m)\varphi(n) = \varphi(d)\varphi(l)$ .



5. 设  $\varphi$  是 Euler 函数.

(i) 证明, 若  $n > 2$ , 则  $\varphi(n)$  是偶数.

(ii) 找出所有满足  $\varphi(n) = 2$  的正整数.

(iii) 找出所有满足  $\varphi(n) = n/p$  的正整数对  $(n, p)$ , 其中  $p$  是一个素数.

6. 证明关于  $\mathbb{Q}$  上分圆多项式  $\Phi_n(X)$  的下列性质:

(i)  $\Phi_p(X) = \Phi_{p^k}(X^{p^{k-1}})$ ,  $p$  是一个素数,  $k > 0$ .

(ii) 设  $n = p_1^{k_1} \cdots p_r^{k_r}$  ( $p_i$  是两两不同的素数,  $k_i > 0$ ,  $1 \leq i \leq r$ ). 则

$$\Phi_n(X) = \Phi_{p_1 \cdots p_r}(X^{p_1^{k_1-1} \cdots p_r^{k_r-1}}).$$

(iii) 如  $n$  是奇数, 则  $\deg \Phi_{2n}(X) = \deg \Phi_n(X)$ .

(iv) 设  $p$  是一个素数且  $p \nmid n$ , 则

$$\Phi_{pn}(X) = \Phi_n(X^p) / \Phi_n(X).$$

(v) 若  $n = p^k$ ,  $p$  是素数,  $k > 0$ , 则  $\Phi_n(1) = p$ ; 在其它情形,  $\Phi_n(1) = 0$ .

7. 写出  $\Phi_{12}(X)$  和  $\Phi_{36}(X)$  的表达式.

### 3.5 分圆扩域

设  $K$  是域  $F$  的一个 Galois 扩域, 如果 Galois 群  $G(K/F)$  是一个 Abel 群, 那么就称  $K$  是  $F$  的一个 **Abel 扩域** ( $K/F$  称为 **Abel 扩张**).

一类重要的 Abel 扩张就是所谓的分圆扩张.

设  $F$  是一个域,  $\Omega$  是  $F$  的代数闭包.  $\Omega/F$  的一个中间域  $K$  叫做  $F$  的一个 **分圆扩域**, 如果  $K$  是通过对  $F$  添加某些单位根而生成的.

根据这个定义, 如果  $K$  是  $F$  的一个分圆扩域, 那么  $K = F(W_K)$ , 这里  $W_K$  是  $K$  所含的一切单位根所成的集.

**定理 3.5.1** 域  $F$  的分圆扩域是 Abel 扩域.

证 设  $K$  是域  $F$  的一个分圆扩域. 首先证明,  $K$  是  $F$  的 Galois 扩域. 令  $W_K$  是  $K$  所含的单位根的全体. 设  $\zeta \in W_K$ ,  $\zeta \neq 1$ . 令  $n$  是  $\zeta$  的阶. 则  $\zeta^n = 1$ , 而对于任意  $1 \leq m \leq n$ ,  $\zeta^m \neq 1$ . 所以  $\text{char } F \nmid n$ . 因此  $X^n - 1$  是  $F[X]$  的一个可分多项式. 所以  $\zeta$  是  $F$  上可分元素. 这样,  $K = F(W_K)$  是  $F$  的可分扩域.

再来证明  $K$  是  $F$  的正规扩域. 设  $K'$  是一个与  $K$  在  $F$  上共轭的域. 那么存在  $K$  与  $K'$  的一个共同的扩域  $M$  和  $K$  到  $K'$  的一个  $F$ -同构  $\sigma$ . 我们有  $K = F(W_K)$ ,  $K' = F(\sigma(W_K))$ , 这里

$$\sigma(W_K) = \{\sigma(\zeta) \mid \zeta \in W_K\}.$$

因为  $\sigma$  是  $K$  到  $K'$  的同构映射, 所以  $\sigma(W_K)$  恰是  $K'$  所含的单位根的全体  $W_{K'}$ . 于是  $K' = F(W_{K'})$ . 设  $\zeta \in W_K$  是  $W_K$  的一个  $n$  阶元素. 则  $\zeta^n = 1$ . 从而  $\sigma(\zeta)^n = 1$ . 所以  $\sigma(\zeta) \in W_{K'}$ . 这样,  $\sigma(\zeta)$  也是一个  $n$  次单位根. 然而  $1, \zeta, \dots, \zeta^{n-1} \in M$  是全部  $n$  次单位根, 所以必有某一个  $i$ ,  $0 \leq i \leq n-1$ , 使得  $\sigma(\zeta) = \zeta^i$ . 所以  $\sigma(\zeta) \in W_K$ , 从而  $W_{K'} = \sigma(W_K) \subseteq W_K$ . 以  $\sigma^{-1}$  代  $\sigma$ , 我们同样地可以得出  $W_K \subseteq W_{K'}$ . 这样  $W_K = W_{K'}$  而  $K = K'$ . 所以  $K$  是  $F$  的 Galois 扩域.

以上证明了  $K/F$  是 Galois 扩张.

现在证明  $K/F$  是 Abel 扩张. 设  $\sigma, \tau \in G(K/F)$ . 由以上的证明可知, 对于任意  $\zeta \in W_K$ , 存在整数  $i$  和  $j$ , 使得  $\sigma(\zeta) = \zeta^i$ ,  $\tau(\zeta) = \zeta^j$ . 于是

$$\sigma\tau(\zeta) = \zeta^{ij} = \tau\sigma(\zeta).$$

由于  $K = F(W_K)$ , 所以对于  $K$  的任意元素  $\alpha$  都有  $\sigma\tau(\alpha) = \tau\sigma(\alpha)$ . 所以  $\sigma\tau = \tau\sigma$ , 即  $G(K/F)$  是 Abel 群. ■

**定理 3.5.2** 设  $K$  是域  $F$  的一个扩域. 对于  $K$  来说, 以下两个条件是等价的:

- (i)  $K$  是  $F$  的有限次分圆扩域;
- (ii) 存在一个本原单位根  $\zeta \in K$ , 使得  $K = F(\zeta)$ .

证 (i)  $\implies$  (ii)  $K = F(W_K)$ . 因为  $[K : F] < \infty$ , 所以总可以选取有限个  $\zeta_1, \dots, \zeta_s \in W_K$ , 使得  $K = F(\zeta_1, \dots, \zeta_s)$ , 这里  $\zeta_i$  是一个本原  $n_i$  次单位根,  $1 \leq i \leq s$ . 令  $n$  是  $n_1, \dots, n_s$  的最小公倍. 由 3.4.1,  $W_K$  含有一个本原  $n$  次单位根  $\zeta$ ; 而  $\zeta_i = \zeta^{m_i}$ , 这里  $m_i$  是某一个正整数,  $1 \leq i \leq s$ . 于是

$$K = F(\zeta_1, \dots, \zeta_s) \subseteq F(\zeta) \subseteq F(W_K) \subseteq K,$$

所以  $K = F(\zeta)$ .

(ii)  $\implies$  (i)  $K = F(\zeta)$  是分圆扩域, 且  $[K : F] < \infty$ . ■

设  $n$  是一个正整数. 令  $\bar{a} = a \bmod n$  是整数  $a$  关于以  $n$  为模的剩余类. 我们知道,

$$\{\bar{a} \mid a \in \mathbb{Z}, (a, n) = 1\}$$

作成剩余类环  $\mathbb{Z}/(n)$  的一个乘法群, 称为以  $n$  为模的不可约剩余类群, 记作  $(\mathbb{Z}/(n))^*$ .

**定理 3.5.3** 设  $n$  不能被域  $F$  的特征整除,  $\zeta$  是一个本原  $n$  次单位根. 那么分圆扩域  $K = F(\zeta)$  的 Galois 群  $G(K/F)$  与  $(\mathbb{Z}/(n))^*$  的一个子群同构.

证  $\zeta \in K$  是一个本原  $n$  次单位根, 因此  $K$  含有全体  $n$  次单位根所成的  $n$  阶循环群  $W_n$ ,  $\zeta$  是  $W_n$  的一个生成元. 设  $\sigma \in G(K/F)$ . 则  $\sigma(\zeta) \in W_n$  也是一个本原  $n$  次单位根, 所以

$$\sigma(\zeta) = \zeta^{v(\sigma)}.$$

这里  $v(\sigma)$  是一个与  $n$  互素的整数. 如果  $m$  是一个整数, 使得  $\sigma(\zeta) = \zeta^m$ , 则

$$m \equiv v(\sigma) \pmod{n}.$$

设  $\sigma, \tau \in G(K/F)$ , 那么

$$\zeta^{v(\sigma\tau)} = \sigma\tau(\zeta) = \zeta^{v(\sigma)v(\tau)}.$$

因此

$$v(\sigma\tau) \equiv v(\sigma)v(\tau) \pmod{n}.$$

这样,

$$\nu: G(K/F) \ni \sigma \mapsto \overline{\nu(\sigma)} \in (\mathbb{Z}/(n))^*$$

是群  $G(K/F)$  到群  $(\mathbb{Z}/(n))^*$  内的同态映射。如果

$$\nu(\sigma) \equiv 1 \pmod{n},$$

则  $\sigma(\zeta) = \zeta$ ; 从而  $\sigma = 1$ , 所以  $\nu$  是单射。这就是说,  $G(K/F)$  与  $(\mathbb{Z}/(n))^*$  的一个子群同构。■

设  $F$  是一个域,  $n$  是一个正整数且  $\text{char } F \nmid n$ 。我们知道, 在  $F$  的一个代数闭包  $\Omega$  内的全体  $n$  次单位根作成 一个  $n$  阶循环群  $W_n$ 。  $K = F(W_n)$  是多项式  $X^n - 1$  在  $F$  上的分裂域。我们有  $K = F(\zeta)$ ,  $\zeta$  是一个本原  $n$  次单位根。由上面所证的定理,  $K/F$  是一个 Galois 扩张而群  $G(K/F)$  与  $(\mathbb{Z}/(n))^*$  的一个子群同构。这个同构是这样建立的:

$$\nu: G(K/F) \ni \sigma \mapsto \overline{\nu(\sigma)} \in (\mathbb{Z}/(n))^*,$$

这里  $\sigma(\zeta) = \zeta^{\nu(\sigma)}$ 。剩余类  $\overline{\nu(\sigma)}$  不依赖于  $W_n$  的生成元  $\zeta$  的选取。事实上, 设  $\zeta'$  也是一个本原  $n$  次单位根。那么  $K = F(\zeta')$ 。我们有  $\zeta' = \zeta^a$ , 这里  $a$  是一个与  $n$  互素的整数。设  $\sigma(\zeta') = \zeta'^{\nu'(\sigma)}$ 。于是

$$\begin{aligned} \zeta'^{\nu'(\sigma)} &= \sigma(\zeta') = \sigma(\zeta^a) = \sigma(\zeta)^a \\ &= \zeta^{a\nu(\sigma)} = \zeta'^{\nu(\sigma)}. \end{aligned}$$

所以

$$\nu'(\sigma) \equiv \nu(\sigma) \pmod{n}.$$

这样, 我们就证明了以下的

**推论 3.5.4** 设  $F$  是一个域,  $n$  是一个正整数且  $\text{char } F \nmid n$ 。多项式  $X^n - 1$  在  $F$  上的分裂域  $K$  是一个 Abel 扩张。Galois 群  $G(K/F)$  与  $(\mathbb{Z}/(n))^*$  的一个子群同构。■

**例 1** 令  $W = \{e^{2k\pi i/n} \mid n=1, 2, \dots; 0 \leq k \leq n-1\}$  是复数域  $\mathbb{C}$  内一切单位根所成的集。  $\mathbb{C}$  的子域  $\mathbb{Q}(W)$  是  $\mathbb{Q}$  的一个无限次的 Abel 扩张。

例 2 令  $F = F_q$  是  $q$  元有限域.  $m \geq 2$  是一个正整数且  $(m, q) = 1$ .  $\zeta$  是一个本原  $m$  次单位根 (含于  $F$  的某一个扩域内). 设  $K = F(\zeta)$ . 则  $W_K = K$ .

$$[K : F] = [F_q(\zeta) : F_q] = f,$$

这里  $f$  是满足

$$q^f \equiv 1 \pmod{m}$$

的最小正指数. 它是群  $(\mathbb{Z}/(m))^*$  中  $q$  所在的剩余类  $\bar{q}$  的阶. 因此  $G(K/F)$  与  $(\mathbb{Z}/(m))^*$  中由  $\bar{q}$  所生成的子群  $\langle \bar{q} \rangle$  同构.

最后, 利用前一节有关的结果, 我们有

**定理 3.5.5** 对有理数域  $\mathbb{Q}$  添加一个本原  $n$  次单位根  $\zeta$  所得的分圆扩域  $K = \mathbb{Q}(\zeta)$  是  $\mathbb{Q}$  的一个  $\varphi(n)$  次 Abel 扩域, 这里  $\varphi(n)$  表示 Euler 函数. Galois 群  $G(K/\mathbb{Q})$  由一切

$$\sigma_a : \zeta \mapsto \zeta^a, \quad (a, n) = 1,$$

组成, 它与以  $n$  为模的不可约剩余类群  $(\mathbb{Z}/(n))^*$  同构.

**证** 定理的前一个断言是 3.5.2 和 3.4.4 的直接结果. 只剩下证明后一个断言. 由 3.5.3,

$$\nu : G(K/\mathbb{Q}) \ni \sigma \mapsto \overline{\nu(\sigma)} \in (\mathbb{Z}/(n))^*$$

是一个群同态单射, 这里  $\sigma(\zeta) = \zeta^{\nu(\sigma)}$ . 另一方面,  $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}/(n))^*|$ . 所以  $\nu$  是满射. ■

为了确定起见, 我们把对有理数域  $\mathbb{Q}$  添加一个本原  $n$  次单位根  $\zeta$  所得的分圆扩域  $\mathbb{Q}(\zeta)$  叫做圆的  $n$  分域.

## 习 题

1. (i) 设  $p$  是一个奇素数. 证明, 不可约剩余类群  $(\mathbb{Z}/(p^n))^*$  是一个阶为  $p^{n-1}(p-1)$  的循环群.

(ii) 当  $p=2, n=1$  或  $2$  时, (i) 也成立.

(iii) 当  $n \geq 3$  时, 不可约剩余类群  $(\mathbb{Z}/(2^n))^*$  是一个二阶循环子群与一个  $2^{n-1}$  阶循环子群的直积.

2. 设  $K/F$  是有限次 Galois 扩张.  $G$  是它的 Galois 群,  $H$  是  $G$  的一个子群,  $E$  是与  $H$  对应的  $K/F$  的中间域. 证明,  $E/F$  是 Abel 扩张当且仅当  $H \supseteq [G, G]$ , 这里  $[G, G]$  表示  $G$  的换位子群.

3. 设  $K_1, K_2$  都是域  $F$  的某一个代数闭包  $\Omega$  的子域, 且  $K_i \supseteq F$  都是 Abel 扩张,  $i=1, 2$ . 证明,  $K_1 K_2$  也是  $F$  的 Abel 扩张.

4. 设  $m, n$  是两个正整数,  $d$  和  $l$  分别是  $m, n$  的最大公约数和最小公倍数. 令  $K_m$  和  $K_n$  分别表示圆的  $m$  分域和  $n$  分域. 证明,  $K_m \cap K_n$  是圆的  $d$  分域,  $K_m K_n$  是圆的  $l$  分域.

5. 令  $K_n = \mathbb{Q}(\zeta)$  是圆的  $n$  分域,  $\zeta$  是一个本原  $n$  次单位根.

(i) 设  $p$  是一个奇素数. 问  $[K_{p^r} : \mathbb{Q}] = ?$

(ii)  $K_2 = \mathbb{Q}, K_4 = \mathbb{Q}(\sqrt{-1})$ .

(iii) 当  $r \geq 3$  时,  $K_{2^r} = \mathbb{Q}(\sqrt{-1})\mathbb{Q}(\cos(\pi/2^{r-1}))$ . 且  $\mathbb{Q}(\sqrt{-1}) \cap \mathbb{Q}(\cos(\pi/2^{r-1})) = \mathbb{Q}$ .

6. 记号同第 5 题.

(i) 确定  $K_5/\mathbb{Q}$  的所有中间域;

(ii) 确定  $K_8/\mathbb{Q}$  的所有中间域;

(iii) 确定  $K_7/\mathbb{Q}$  的所有中间域. 设  $\zeta$  是一个本原 7 次单位根, 求  $\zeta + \zeta^{-1}$  在  $\mathbb{Q}$  上的最小多项式.

7. 设  $n > 2$ ,  $\zeta$  是一个本原  $n$  次单位根. 则  $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$ .

### 3.6 范和迹

我们以下将讨论另一类重要的 Abel 扩张, 这种扩张的 Galois 群是循环群, 为此, 在这一节里, 先介绍范和迹的概念, 这两个概念本身也是重要的.

设  $K$  是域  $F$  的一个有限次扩域,  $\Omega$  是  $F$  的一个包含  $K$  的代数闭包. 令  $\sigma_1, \dots, \sigma_m$  是  $K$  到  $\Omega$  内的一切互不相同的  $F$ -共轭. 对于  $\alpha \in K$ , 定义

$$N_F^K(\alpha) = \left( \prod_{j=1}^m \sigma_j(\alpha) \right)^{[K:F]},$$

称为  $\alpha$  的范. 定义

$$T_F^K(\alpha) = [K:F] \sum_{j=1}^m \sigma_j(\alpha),$$

称为  $\alpha$  的迹.

下面我们即将看到, 范和迹都是域  $F$  的元素 (见 3.6.2), 因而不依赖于代数闭包  $\Omega$  的选取. 当  $K/F$  是可分扩张时,  $[K:F]_i = 1$ , 在不致引起混淆的情况下, 我们这时将  $N_F^K$  和  $T_F^K$  分别简写作  $N$  和  $T$ :

$$N(\alpha) = \prod_{j=1}^m \sigma_j(\alpha); \quad T(\alpha) = \sum_{j=1}^m \sigma_j(\alpha).$$

**例 1** 设  $K = \mathbb{C}$ ,  $F = \mathbb{R}$ ,  $\Omega = \mathbb{C}$ . 那么  $K$  到  $\mathbb{C}$  内的  $\mathbb{R}$ -共轭只有两个. 即  $\mathbb{C}$  的恒等自同构  $1_\sigma$  和对合  $\sigma: a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$  ( $a, b \in \mathbb{R}$ ). 于是

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2;$$

$$T(a + bi) = (a + bi) + (a - bi) = 2a.$$

**例 2** 设  $\text{char } F = p > 0$ ,  $K = F(\alpha)$  是一个  $n$  次单扩域,  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式,  $\Omega$  是  $K$  的一个代数闭包,  $m$  是  $f(X)$  的可分次数,  $p^e$  是  $f(X)$  的不可分次数. 那么在  $\Omega[X]$  内,

$$f(X) = (X - \alpha_1)^{p^e} \cdots (X - \alpha_m)^{p^e},$$

$\alpha_1, \dots, \alpha_m$  两两不同,  $\alpha = \alpha_1$ . 于是

$$N_F^K(\alpha) = \left( \prod_{j=1}^m \alpha_j \right)^{p^e};$$

$$T_F^K(\alpha) = p^\alpha \cdot \sum_{j=1}^m \alpha_j.$$

特别, 如果  $\alpha$  是可分元素, 则  $T_F^K(\alpha)$  就是  $f(X)$  中  $X^{n-1}$  的系数改变符号.  $N_F^K(\alpha)$  就是  $f(X)$  的常数项乘以  $(-1)^n$ .

**定理 3.6.1** 设  $K$  是域  $F$  的一个有限次 Galois 扩域,  $G(K/F) = \{\sigma_1, \dots, \sigma_m\}$ , 那么对于任意  $\alpha \in K$ ,

$$N_F^K(\alpha) = \prod_{j=1}^m \sigma_j(\alpha);$$

$$T_F^K(\alpha) = \sum_{j=1}^m \sigma_j(\alpha).$$

**证** 取定  $K$  的一个代数闭包  $\Omega$ . 因为  $K/F$  是 Galois 扩张, 所以  $\sigma_1, \dots, \sigma_m$  就是  $K$  到  $\Omega$  内的全部  $F$ -共轭. 又因为  $K/F$  是可分的, 所以  $[K:F]_i = 1$ . ■

**定理 3.6.2** 设  $K$  是域  $F$  的一个有限次扩域.  $\alpha, \beta \in K$ .

(i)  $N_F^K(\alpha\beta) = N_F^K(\alpha)N_F^K(\beta)$ ;  $T_F^K(\alpha + \beta) = T_F^K(\alpha) + T_F^K(\beta)$ .

(ii) 如果  $\alpha \in F$ , 则

$$N_F^K(\alpha) = \alpha^{[K:F]}; \quad T_F^K(\alpha) = [K:F]\alpha.$$

(iii) 设  $f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in F[X]$  是  $\alpha$  在  $F$  上的最小多项式. 则

$$N_F^K(\alpha) = ((-1)^n a_n)^{[K:F(\alpha)]};$$

$$T_F^K(\alpha) = -[K:F(\alpha)]a_1.$$

因此,  $N_F^K(\alpha), T_F^K(\alpha) \in F$ .

(iv) 设  $E$  是  $K/F$  的一个中间域. 则

$$N_E^K(N_F^K(\alpha)) = N_F^K(\alpha); \quad T_E^K(T_F^K(\alpha)) = T_F^K(\alpha).$$

(由 (iii),  $N_E^K(\alpha), T_E^K(\alpha) \in E$ ).

**证** (i) 直接由定义得出.

(ii) 因为  $[K:F] = [K:E][E:F]$ , 再根据 2.8.5,



即可得出(ii).

(iii) 令  $E = F(\alpha)$ ,  $F \subseteq E \subseteq K$ . 取定  $F$  的一个包含  $K$  的代数闭包. 设  $\{\sigma_1, \dots, \sigma_m\}$  是一切  $E$  到  $\Omega$  内的  $F$ -共轭,  $\{\tau_1, \dots, \tau_l\}$  是一切  $K$  到  $\Omega$  内的  $E$ -共轭. 由 2.6.1,

$$\{\sigma_k \tau_j \mid 1 \leq k \leq m, 1 \leq j \leq l\}$$

是一切  $K$  到  $\Omega$  内的  $F$ -共轭. 由 2.8.5,  $[K : E]_s = l$ , 而

$$[K : E] = [K : E]_s [K : E]_i = l [K : E]_i.$$

又由 2.8.6,  $[K : F]_i = [K : E]_i [E : F]_i$ . 因为  $\alpha \in E$ , 所以

$$\begin{aligned} N_F^K(\alpha) &= \left( \prod_{k=1}^m \prod_{j=1}^l \sigma_k \tau_j(\alpha) \right)^{[K : F]_i} \\ &= \left( \prod_{k=1}^m \sigma_k(\alpha)^l \right)^{[K : F]_i} \\ &= \left( \prod_{k=1}^m \sigma_k(\alpha) \right)^{l [K : E]_i [E : F]_i} \\ &= \left( \prod_{k=1}^m \sigma_k(\alpha) \right)^{[K : E] [E : F]_i}. \end{aligned}$$

同样地,

$$T_F^K(\alpha) = [K : E] [E : F]_i \sum_{k=1}^m \sigma_k(\alpha).$$

因为  $\sigma_i : E = F(\alpha) \rightarrow F(\sigma_i(\alpha))$  是  $E$  到  $\Omega$  内的  $F$ -共轭, 由 2.2.7,  $\sigma_1(\alpha), \dots, \sigma_m(\alpha)$  恰是  $f(X)$  的一切互不相同的根. 所以

$$\begin{aligned} f(X) &= \left( \prod_{k=1}^m (X - \sigma_k(\alpha)) \right)^{[E : F]_i} \\ &= \left( X^m - \sum_{k=1}^m \sigma_k(\alpha) X^{m-1} + \dots + \right. \\ &\quad \left. + (-1)^m \prod_{k=1}^m \sigma_k(\alpha) \right)^{[E : F]_i} \end{aligned}$$

如果  $[E : F]_i = 1$ , 则  $m = n$ , 这时 (iii) 成立. 设  $[E : F]_i =$

$= p^f > 1$ ,  $p = \text{char } F$ ,  $f > 0$ . 那么

$$a_n = (-1)^{mp^f} \left( \prod_{k=1}^m \sigma_k(\alpha) \right)^{p^f} = (-1)^n \left( \prod_{k=1}^m \sigma_k(\alpha) \right)^{p^f}$$

而

$$N_F^K(\alpha) = \left( \prod_{k=1}^m \sigma_k(\alpha) \right)^{p^f} [K : E] = \left( (-1)^n a_n \right)^{[K : E]}$$

在这个情况下,  $a_1 = 0$ , 而

$$T_F^K(\alpha) = p^f [K : E] \sum_{k=1}^m \sigma_k(\alpha) = 0,$$

所以(iii)成立.

(iv) 记号同(iii). 我们有

$$N_E^K(\alpha) = \left( \prod_{j=1}^l \tau_j(\alpha) \right)^{[K : E]_i} \in E.$$

于是

$$\begin{aligned} N_F^E(N_E^K(\alpha)) &= N_F^E \left( \left( \prod_{j=1}^l \tau_j(\alpha) \right)^{[K : E]_i} \right) \\ &= \left( N_F^E \left( \prod_{j=1}^l \tau_j(\alpha) \right) \right)^{[K : E]_i} \\ &= \left( \prod_{k=1}^m \prod_{j=1}^l \sigma_k \tau_j(\alpha) \right)^{[E : F]_i [K : E]_i} \\ &= \left( \prod_{k=1}^m \prod_{j=1}^l \sigma_k \tau_j(\alpha) \right)^{[K : F]_i} = N_F^K(\alpha). \end{aligned}$$

另一方面,

$$T_E^K(\alpha) = [K : E]_i \sum_{j=1}^l \tau_j(\alpha) \in E.$$

所以

$$T_F^E(T_E^K(\alpha)) = [K : E]_i [E : F]_i \sum_{k=1}^m \sigma_k \left( \sum_{j=1}^l \tau_j(\alpha) \right)$$

$$=[K:F], \sum_{k=1}^m \sum_{j=1}^l \sigma_k \tau_j(\alpha) = T_F^K(\alpha). \quad \blacksquare$$

## 习 题

1. 证明, 在范和迹的定义里, 取  $F$  的一个包含  $K$  的正规扩域  $N$  来代替  $\Omega$ , 这样定义的范和迹与原来的定义是等价的. 并且这个定义不依赖于  $N$  的选取.

2. 设  $F = F_q$  是一个  $q$  元有限域,  $K$  是  $F$  的一个有限次扩域. 证明:

$$N : K \ni \alpha \mapsto N_F^K(\alpha) \in F,$$

$$T : K \ni \alpha \mapsto T_F^K(\alpha) \in F$$

都是  $K$  到  $F$  的满射.

3. 设  $K$  是域  $F$  上一个有限次可分扩域. 对于任意  $\alpha, \beta \in K$ , 定义

$$B(x, y) = T(\alpha\beta).$$

证明,  $B : K \times K \rightarrow F$  是一个非退化对称双线性函数.

4. 设  $K$  是域  $F$  上一个  $n$  次可分扩域. 证明,  $K$  中  $n$  个元素  $\alpha_1, \alpha_2, \dots, \alpha_n$  构成  $K$  在  $F$  上一个基必要且只要  $n \times n$  矩阵  $(B(\alpha_i, \alpha_j))_{i,j=1}^n$  非退化, 这里  $B$  是第三题所定义的双线性函数.

5. 设  $K/F$  是一个  $n$  次可分扩张,  $\alpha_1, \dots, \alpha_n$  是  $K$  在  $F$  上一个基. 行列式  $\det(B(\alpha_i, \alpha_j))$  叫做  $K/F$  的判别式. 这里  $B(\alpha_i, \alpha_j) = T(\alpha_i \alpha_j)$ ,  $i, j = 1, 2, \dots, n$ .

(i) 证明. 如果  $\beta_1, \dots, \beta_n$  也是  $K$  在  $F$  上一个基, 则  $\det(B(\beta_i, \beta_j)) = c^2 \det(B(\alpha_i, \alpha_j))$ , 这里  $c$  是  $F$  中一个非零元素.

(ii) 设  $K = F(\alpha)$  是单扩域. 对于基  $1, \alpha, \dots, \alpha^{n-1}$ , 计算  $K/F$  的判别式.

### 3.7 循环扩域

设  $F$  是一个域,  $K$  是  $F$  的一个 Galois 扩域. 如果 Galois 群  $G(K/F)$  是一个循环群, 那么就称  $K$  是  $F$  的一个循环扩域, 相应地,  $K/F$  称为循环扩张.

关于循环扩张的信息是清楚的. 我们先做一点准备工作.

**引理 3.7.1** 设  $K$  是一个域,  $S$  是  $K$  的一些自同构所组成的集. 则  $S$  在  $K$  上线性无关.

**证** 如果存在  $\sigma_1, \dots, \sigma_m \in S$  和  $K$  中不全为零的元素  $a_1, \dots, a_m$ , 使得对于任意  $\alpha \in K$  来说, 都有

$$(1) \quad a_1 \sigma_1(\alpha) + \dots + a_m \sigma_m(\alpha) = 0.$$

可设  $m$  是  $S$  中满足这样线性关系的元素的最小个数. 显然  $m > 1$ . 因为  $\sigma_1 \neq \sigma_2$ , 所以存在  $\beta \in K$ , 使得  $\sigma_1(\beta) \neq \sigma_2(\beta)$ . 对于任意  $\alpha \in K$ , 我们有

$$\begin{aligned} & a_1 \sigma_1(\alpha) \sigma_1(\beta) + a_2 \sigma_2(\alpha) \sigma_2(\beta) + \dots + a_m \sigma_m(\alpha) \sigma_m(\beta) \\ &= a_1 \sigma_1(\alpha\beta) + a_2 \sigma_2(\alpha\beta) + \dots + a_m \sigma_m(\alpha\beta) = 0. \end{aligned}$$

另一方面, 用  $\sigma_1(\beta)$  乘(1)式得

$$\begin{aligned} & a_1 \sigma_1(\alpha) \sigma_1(\beta) + a_2 \sigma_2(\alpha) \sigma_1(\beta) + \dots \\ &+ a_m \sigma_m(\alpha) \sigma_1(\beta) = 0. \end{aligned}$$

把这两个式子相减得

$$\begin{aligned} & a_2 (\sigma_2(\beta) - \sigma_1(\beta)) \sigma_2(\alpha) + \dots \\ &+ a_m (\sigma_m(\beta) - \sigma_1(\beta)) \sigma_m(\alpha) = 0. \end{aligned}$$

因为  $a_2 \neq 0$ ,  $\sigma_2(\beta) - \sigma_1(\beta) \neq 0$ , 这样一来就得到  $S$  中元素的一个更短的线性关系. 与  $m$  的最小性矛盾. ■

**引理 3.7.2** 设  $K$  是域  $F$  的一个  $n$  次循环扩域,  $\sigma$  是 Galois 群  $G(K/F)$  的一个生成元. 对于  $K$  中的元素  $\alpha$ ,

$$(i) \quad T_F^K(\alpha) = 0 \iff \text{存在 } \beta \in K \text{ 使得 } \alpha = \beta - \sigma(\beta).$$

$$(ii) \quad N_F^K(\alpha) = 1 \iff \text{存在 } \beta \in K, \beta \neq 0 \text{ 使得 } \alpha = \beta \sigma(\beta)^{-1}.$$

证  $G(K/F) = \{1 = \sigma^n, \sigma, \dots, \sigma^{n-1}\}$ . 我们有

$$T(\alpha) = T_F^K(\alpha) = \alpha + \sigma(\alpha) + \dots + \sigma^{n-1}(\alpha),$$

$$N(\alpha) = N_F^K(\alpha) = \alpha \sigma(\alpha) \dots \sigma^{n-1}(\alpha).$$

(i) 如果存在  $\beta \in K$ , 使得  $\alpha = \beta - \sigma(\beta)$ , 则

$$\begin{aligned} T(\alpha) &= T(\beta - \sigma(\beta)) = \beta + \sigma(\beta) + \dots + \sigma^{n-1}(\beta) \\ &\quad - \sigma(\beta) - \dots - \sigma^{n-1}(\beta) - \sigma^n(\beta) = 0. \end{aligned}$$

反之, 设  $T(\alpha) = 0$ . 我们可以如下地选取  $\gamma \in K$ , 使得  $T(\gamma) = 1$ . 首先, 由 3.7.1,  $1, \sigma, \dots, \sigma^{n-1}$  在  $K$  上线性无关, 所以  $1 + \sigma + \dots + \sigma^{n-1} \neq 0$ . 因此存在  $\delta \in K$ , 使得

$$T(\delta) = \delta + \sigma(\delta) + \dots + \sigma^{n-1}(\delta) \neq 0.$$

由 3.6.2 (iii),  $T(\delta) \in F$ , 所以  $T(\delta)^{-1} \in F$ . 从而  $\sigma(T(\delta)^{-1} \delta) = T(\delta)^{-1} \sigma(\delta)$ . 取  $\gamma = T(\delta)^{-1} \delta \in K$ . 那么

$$\begin{aligned} T(\gamma) &= T(\delta)^{-1} \delta + T(\delta)^{-1} \sigma(\delta) + \dots + T(\delta)^{-1} \sigma^{n-1}(\delta) \\ &= T(\delta)^{-1} T(\delta) = 1. \end{aligned}$$

现在取

$$\begin{aligned} \beta &= \alpha \gamma + (\alpha + \sigma(\alpha)) \sigma(\gamma) + (\alpha + \sigma(\alpha) + \sigma^2(\alpha)) \sigma^2(\gamma) + \dots \\ &\quad + (\alpha + \sigma(\alpha) + \dots + \sigma^{n-2}(\alpha)) \sigma^{n-2}(\gamma). \end{aligned}$$

则

$$\begin{aligned} \sigma(\beta) &= \sigma(\alpha) \sigma(\gamma) + (\sigma(\alpha) + \sigma^2(\alpha)) \sigma^2(\gamma) + (\sigma(\alpha) + \\ &\quad + \sigma^2(\alpha) + \sigma^3(\alpha)) \sigma^3(\gamma) + \dots + \\ &\quad + (\sigma(\alpha) + \sigma^2(\alpha) + \dots + \sigma^{n-1}(\alpha)) \sigma^{n-1}(\gamma). \end{aligned}$$

因为  $T(\alpha) = 0$ , 所以  $\sigma(\alpha) + \dots + \sigma^{n-1}(\alpha) = -\alpha$ . 于是

$$\begin{aligned} \beta - \sigma(\beta) &= \alpha \gamma + \alpha \sigma(\gamma) + \alpha \sigma^2(\gamma) + \dots + \\ &\quad + \alpha \sigma^{n-2}(\gamma) + \alpha \sigma^{n-1}(\gamma) \\ &= \alpha(\gamma + \sigma(\gamma) + \dots + \sigma^{n-1}(\gamma)) = \alpha T(\gamma) = \alpha. \end{aligned}$$

(ii) 如果  $\alpha = \beta \sigma(\beta)^{-1}$ , 那么  $\sigma^j(\alpha) = \sigma^j(\beta) \sigma^{j+1}(\beta)^{-1}$ , 而  $\sigma^n(\beta)^{-1} = \beta^{-1}$ , 所以

$$N(\alpha) = \prod_{j=0}^{n-1} \sigma^j(\alpha) = \prod_{j=0}^{n-1} \sigma^j(\beta) \sigma^{j+1}(\beta)^{-1} = \beta \beta^{-1} = 1.$$

反之, 设  $N(\alpha) = 1$ , 则  $\alpha \neq 0$ . 因为  $1, \sigma, \dots, \sigma^{n-1}$  线性无关, 所以存在  $\eta \in K$ , 使得

$$\begin{aligned} \beta &= \alpha \eta + \alpha \sigma(\alpha) \sigma(\eta) + \alpha \sigma(\alpha) \sigma^2(\alpha) \sigma^2(\eta) + \dots \\ &\quad + \alpha \sigma(\alpha) + \dots \sigma^{n-1}(\alpha) \sigma^{n-1}(\eta) \neq 0. \end{aligned}$$

又  $\alpha \sigma(\alpha) \dots \sigma^{n-1}(\alpha) \sigma^{n-1}(\eta) = N(\alpha) \sigma^{n-1}(\eta) = \sigma^{n-1}(\eta)$ . 所以

$$\begin{aligned} \alpha^{-1} \beta &= \eta + \sigma(\alpha) \sigma(\eta) + \dots + \sigma(\alpha) \dots \sigma^{n-2}(\alpha) \sigma^{n-2}(\eta) + \\ &\quad + \sigma(\alpha) \dots \sigma^{n-1}(\alpha) \sigma^{n-1}(\eta) = \sigma(\beta). \end{aligned}$$

所以  $\alpha = \beta \sigma(\beta)^{-1}$ . ■

现在我们来研究有限次循环扩域的构造. 先证明

**定理 3.7.3** 设  $F$  是一个域且  $\text{char } F = p > 0$ ,  $K$  是  $F$  的一个  $n$  次循环扩域. 如果  $n = mp^f$ ,  $(m, p) = 1$ ,  $f \geq 0$ , 那么存在一串中间域

$$K \supseteq E_0 \supseteq E_1 \supseteq \dots \supseteq E_f = F,$$

其中  $K$  是  $E_0$  的一个  $m$  次循环扩域, 而  $E_{i-1}$  是  $E_i$  的一个  $p$  次循环扩域,  $1 \leq i \leq f$  (若  $f > 0$ ).

**证** 因为  $G = G(K/F)$  是循环群, 所以  $G$  的每一个子群都是正规的; 又因为  $G$  的每一个子群和每一个同态像都是循环群, 所以对于  $K/F$  的每一个中间域  $E$  来说,  $K/E$  和  $E/F$  都是循环扩张. 由此容易推出, 对于  $K/F$  的任意两个中间域  $L, M$ , 如果  $F \subseteq L \subseteq M \subseteq K$ , 则  $M/L$  是循环扩张.

$G$  有唯一的  $m$  阶循环子群  $H$ . 令  $E_0 = \Phi(H)$  是  $H$  的固定域, 则  $H = G(K/E_0)$ ,  $K$  是  $E_0$  的一个  $m$  次循环扩域, 而  $E_0$  是  $F$  的一个  $p^f$  次循环扩域. 因为  $G(E_0/F)$  是一个  $p^f$  阶循环群, 所以有一个正规子群链,

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{f-1} \triangleleft G_f = G(E_0/F),$$

这里  $|G_i| = p^i$ ,  $(G_i : G_{i-1}) = p$ ,  $i = 1, \dots, f$ . 令

$$E_i = \{\alpha \in E_0 \mid \sigma(\alpha) = \alpha, \forall \sigma \in G_i\}$$

是  $G_i$  的固定域。由基本定理，我们有

$$(a) \quad E_0 \supseteq E_1 \supseteq \cdots \supseteq E_{f-1} \supseteq E_f = F;$$

$$(b) \quad [E_{i-1} : E_i] = (G_i : G_{i-1}) = p;$$

$$(c) \quad G(E_{i-1}/E_i) \cong G_i/G_{i-1}.$$

所以  $E_{i-1}$  是  $E_i$  的一个  $p$  次循环扩域,  $i = 1, \dots, f$ . ■

由于这个定理，对于一个  $n$  次循环扩域的讨论可以归结为以下两个情形：

情形 1  $n = \text{char } F = p > 0$ .

情形 2  $\text{char } F = 0$  或  $\text{char } F = p > 0$  但  $(p, n) = 1$ .

在情形 1，循环扩域的结构由以下定理完全解决。

**定理 3.7.4** 设  $\text{char } F = p > 0$ .  $K$  是  $F$  的一个  $p$  次循环扩域当且仅当  $K$  是  $F$  上一个形如  $X^p - X - a$  的不可约多项式的分裂域，这时  $K = F(\alpha)$ ,  $\alpha$  是  $X^p - X - a$  的任意一个根。

**证** 设  $K/F$  是  $p$  次循环扩张,  $G = G(K/F)$  是一个  $p$  阶循环群. 令  $\sigma$  是  $G$  的一个生成元. 由 3.6.2(ii),  $T_F^K(1) = [K : F] \cdot 1 = p \cdot 1 = 0$ . 于是由 3.7.2(i), 存在  $\beta \in K$ , 使得  $\beta - \sigma(\beta) = 1$ . 令  $\alpha = -\beta$ . 则  $\sigma(\alpha) = \alpha + 1 \neq \alpha$ . 所以  $\alpha \notin F$ . 因为  $[K : F] = p$ , 所以  $K/F$  没有真中间域. 因此必须  $K = F(\alpha)$ . 然而  $\sigma(\alpha^p) = \sigma(\alpha)^p = \alpha^p + 1$ , 所以  $\sigma(\alpha^p - \alpha) = \alpha^p - \alpha$ . 所以  $a = \alpha^p - \alpha \in F$ . 这样,  $\alpha$  是  $F$  上多项式  $f(X) = X^p - X - a$  的一个根. 因为  $\deg(f(X)) = p = [K : F]$ , 所以  $f(X)$  在  $F[X]$  中不可约.

令  $j \in F_p$ ,  $F_p$  是  $F$  的素域. 则  $j^p = j$ . 于是

$$(\alpha + j)^p - (\alpha + j) - a = \alpha^p - \alpha - a = 0.$$

所以  $\alpha + j \in K$  也是  $f(X)$  的根,  $j = 0, 1, \dots, p-1$ . 如果  $i, j \in F_p$ ,  $i \neq j$ , 则  $\alpha + i \neq \alpha + j$ . 这样一来,  $\alpha + j$ ,  $j = 0, 1, \dots, p-1$  恰是  $f(X)$  的全部根, 它们都属于  $K$ , 因此,  $K = F(\alpha)$  是  $f(X)$  在  $F$  上的分裂域.

最后, 显然  $F(\alpha) = F(\alpha + j)$ ,  $j = 0, 1, \dots, p-1$ .

反过来, 设  $K$  是  $f(X) = X^p - X - a \in F[X]$  在  $F$  上的分裂域. 我们先不要求  $f(X)$  在  $F[X]$  中不可约. 设  $\alpha \in K$  是  $f(X)$  的一个根. 由上一段的证明, 我们看到,  $F(\alpha)$  包含  $f(X)$  的全部根  $\alpha + j$ ,  $j = 0, 1, \dots, p-1$ , 这些根两两不同. 所以  $K = F(\alpha)$  是  $F$  的可分正规扩域, 因而是 Galois 扩域.  $G = G(K/F)$  的每一个元素  $\tau$  由它在  $\alpha$  上的作用完全确定.  $\tau(\alpha) = \alpha + j$  对某一个  $j \in F_p$ , 如果  $\tau, \tau' \in G$ ,  $\tau(\alpha) = \alpha + j$ ,  $\tau'(\alpha) = \alpha + j'$ , 那么  $\tau\tau'(\alpha) = \alpha + j + j'$ . 因此,

$$\theta: G \ni \tau \mapsto j \in F_p, \text{ 若 } \tau(\alpha) = \alpha + j,$$

是群  $G$  到以  $p$  为模的剩余类加群  $F_p = \mathbb{Z}/(p)$  的一个同态单射. 于是  $G \cong \text{Im } \theta \subseteq \mathbb{Z}/(p)$ . 因为  $p$  是一个素数, 所以  $\text{Im } \theta = \{1\}$  或  $\text{Im } \theta = \mathbb{Z}/(p)$ . 如果是前者, 则  $G = \{1\}$  而  $[K:F] = 1$ , 从而  $\alpha \in F$ . 这时  $f(X)$  在  $F[X]$  内已经完全分解成线性因式的乘积. 这样, 如果  $f(X)$  在  $F[X]$  中不可约, 必须  $G \cong \mathbb{Z}/(p)$ , 这时  $G$  是一个  $p$  阶循环群. ■

**推论 3.7.5** 设  $F$  是一个特征为  $p > 0$  的域. 那么多项式  $f(X) = X^p - X - a \in F[X]$  或者不可约, 或者在  $F[X]$  中完全分解成线性因式的乘积.

**证** 设  $f(X)$  在  $F[X]$  中不能分解成线性因式的乘积. 令  $\alpha$  是  $f(X)$  在  $F$  的某一个代数闭包  $\Omega$  内的一个根. 且  $\alpha \notin F$ . 那么由 3.7.4,  $K = F(\alpha)$  是一个  $p$  次循环扩域. 这样一来,  $f(X)$  就是  $\alpha$  在  $F$  上的最小多项式; 因而  $f(X)$  不可约. ■

现在我们来讨论情形 2. 这时要对基础域  $F$  作一点限制, 即要求  $F$  含有一个本原  $n$  次单位根.

注意由 3.4.1, (iv), 如果  $F$  含有一个本原  $n$  次单位根, 必须有  $\text{char } F = 0$  或  $\text{char } F = p$ , 而  $p \nmid n$ . 因此只能是情形 2.

我们先证明一个引理.



**引理 3.7.6** 设  $n$  是一个正整数, 域  $F$  含有一个本原  $n$  次单位根  $\zeta$ . 如果  $d$  是  $n$  的一个正因子而  $\alpha \neq 0$  是  $F$  上多项式  $X^d - a$  的一个根. 那么  $X^d - a$  有  $d$  个两两不同的根,  $\alpha, \eta\alpha, \dots, \eta^{d-1}\alpha$ , 这里  $\eta$  是一个本原  $d$  次单位根, 而  $K = F(\alpha)$  是多项式  $X^d - a$  在  $F$  上的分裂域, 并且是  $F$  的一个 Galois 扩域.

**证** 因为  $F$  含有一个本原  $n$  次单位根  $\zeta$ , 而  $d|n$ , 所以  $\eta = \zeta^{n/d} \in F$  是一个本原  $d$  次单位根. 设  $\alpha \neq 0$  是  $X^d - a \in F[X]$  的一个根. 那么  $\alpha, \eta\alpha, \dots, \eta^{d-1}\alpha$  是  $X^d - a$  在  $F(\alpha)$  里的一切根, 且两两不同. 因此,  $F(\alpha)$  是可分多项式  $X^d - a$  在  $F$  上的分裂域, 因而是  $F$  的一个 Galois 扩域. ■

**定理 3.7.7** 设  $n$  是一个正整数. 域  $F$  含有一个本原  $n$  次单位根  $\zeta$ . 对于  $F$  的一个扩域  $K$  来说, 以下三个条件是等价的:

(i)  $K$  是  $F$  上一个形如  $X^d - b$  的不可约多项式在  $F$  上的分裂域, 其中  $d|n$ . 这时  $K = F(\beta)$ ,  $\beta$  是  $X^d - b$  的任意一个根.

(ii)  $K$  是  $F$  上一个形如  $X^n - a$  的多项式在  $F$  上的分裂域. 这时  $K = F(\alpha)$ ,  $\alpha$  是  $X^n - a$  的任意一个根.

(iii)  $K$  是  $F$  的一个  $d$  次循环扩域, 其中  $d|n$ .

**证** (i)  $\implies$  (ii) 设  $\alpha$  是  $F$  上不可约多项式  $X^d - b$  在  $K$  中的一个根,  $d|n$ . 由 3.7.6,  $K = F(\alpha)$  是  $X^d - b$  在  $F$  上的分裂域. 又  $(\zeta\alpha)^n = \alpha^n = b^{n/d} \in F$ . 令  $a = b^{n/d}$ . 则  $\zeta\alpha$  是  $X^n - a \in F[X]$  在  $K$  中的根. 再由 3.7.6,  $F(\zeta\alpha)$  是  $X^n - a$  在  $F$  上的分裂域. 然而  $\zeta \in F$ , 所以  $F(\zeta\alpha) = F(\alpha) = K$ , 并且  $\zeta^i\alpha$  ( $0 \leq i \leq n-1$ ) 就是  $X^n - a$  的全部根, 它们都属于  $K$ .  $K = F(\zeta^i\alpha)$ ,  $i = 0, 1, \dots, n-1$ .

(ii)  $\implies$  (iii)  $K$  是多项式  $X^n - a \in F[X]$  在  $F$  上的分裂域. 令  $\alpha \in K$  是  $X^n - a$  的任意一个根. 由 3.7.6,  $K = F(\alpha)$  是 Galois 扩域, 而  $\alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha$  是  $X^n - a$  的全部根. 设  $\sigma \in (K/F)$ . 那么  $\sigma(\alpha) = \zeta^i\alpha$ , 对某一个  $i$ ,  $0 \leq i \leq n-1$ .

$$\theta: G \ni \sigma \mapsto \zeta^i \in W_n, \text{ 若 } \sigma(\zeta) = \zeta^i,$$

这里  $W_n = \{1, \zeta, \dots, \zeta^{n-1}\}$  是  $n$  次单位根群. 则  $\theta$  是一个群同态单射. 因而  $G$  与  $n$  阶循环群  $W_n$  的一个子群同构, 所以  $G$  是一个  $d$  阶循环群, 这里  $d$  是  $n$  的一个因子.

(iii)  $\implies$  (i)  $G = G(K/F)$  是一个  $d$  阶循环群,  $d|n$ . 令  $\sigma$  是  $G$  的一个生成元.  $\eta = \zeta^{n/d} \in F$  是一个本原  $d$  次单位根. 因为  $N_K^F(\eta) = \eta^{[K:F]} = \eta^d = 1$ , 由 3.7.2, 存在  $\beta \in K$ , 使得  $\eta = \beta\sigma(\beta)^{-1}$ . 令  $\alpha = \beta^{-1}$ . 则  $\sigma(\alpha) = \eta\alpha$ ,  $\sigma(\alpha^d) = (\eta\alpha)^d = \alpha^d$ . 所以  $\alpha^d = b \in F$ . 因此  $\alpha$  是  $F$  上多项式  $X^d - b$  的一个根. 由 3.7.6,  $F(\alpha) \subseteq K$  是  $X^d - b$  在  $F$  上的分裂域,  $\alpha, \eta\alpha, \dots, \eta^{d-1}\alpha$  是  $X^d - b$  的全部根, 并且都属于  $K$ . 对于每一个  $i$ ,  $0 \leq i \leq d-1$ ,  $\sigma^i(\alpha) = \eta^i\alpha$ , 所以  $\sigma^i: F(\alpha) \rightarrow F(\eta^i\alpha)$  是  $F$ -同构. 由 2.2.7,  $\alpha$  与  $\eta^i\alpha$  是  $F$  上同一个不可约多项式的根,  $0 \leq i \leq d-1$ . 这样,  $X^d - b$  是  $F$  上不可约多项式. 所以  $[F(\alpha):F] = d = [K:F]$ ,  $K = F(\alpha)$ .

**注意** 在上面定理 3.7.7 的证明里, 基础域  $F$  含有一个本原  $n$  次单位根这一条件起着重要的作用. 当  $F$  上不含本原  $n$  次单位根时, 对多项式  $X^n - a \in F[X]$  在  $F$  上的分裂域的刻画要困难得多. 当  $a=1$  时, 就是前一节所讨论的分圆扩域.

## 习 题

1. 设  $F$  是一个域,  $\text{char } F \neq 2$ . 又设  $a \in F$  而  $b = 1 + a^2 \in F^2$ . 证明,  $K = F(\sqrt{b + \sqrt{b}}, \sqrt{b - \sqrt{b}})$  是  $F$  的四次循环扩域, 它的 Galois 群由  $K$  的  $F$ -自同构

$$\sigma: \sqrt{b + \sqrt{b}} \mapsto \sqrt{b - \sqrt{b}}$$

生成.

2. 设  $F$  是一个域. 又设存在  $b, c \in F$  使得  $a = b^2 + c^2 \in F^2$ , 证明,  $K = F(\sqrt{a + b}\sqrt{a})$  是  $F$  的四次循环扩域. 求出它的 Galois 群的一个生成元.

3. 令  $\overline{Q}$  是域  $Q$  的一个固定的代数闭包,  $\alpha \in \overline{Q}$  但  $\alpha \notin Q$ . 设

$E$  是  $\overline{Q}$  中不含  $\alpha$  的最大子域。证明,  $E$  的每一个有限次扩域都是循环扩域。

4. 设  $F$  是一个域,  $\Omega$  是  $F$  的一个代数闭包,  $\sigma \in G(\Omega/F)$ . 令

$$K = \{\alpha \in \Omega \mid \sigma(\alpha) = \alpha\}.$$

证明,  $K$  是一个域, 并且  $K$  的每一个有限次扩域都是循环扩域。

5. 设  $p$  是一个素数,  $K$  是域  $F$  的一个  $p^n$  次循环扩域,  $E \subset K$  并且是  $F$  的  $p^{n-1}$  次循环扩域。又设  $\alpha \in K$  使得  $K = E(\alpha)$ 。证明,  $K = F(\alpha)$ 。

6. 设  $p$  是一个素数,  $F$  是一个域。

(i) 如果  $\text{char } F = p$ , 或者  $\text{char } F \neq p$ , 但  $F$  含有一个本原  $p$  次单位根, 那么  $X^p - a \in F[X]$  或者不可约, 或者在  $F[X]$  内可以分解成一次因式的积。

(ii) 设  $\text{char } F = p$ , 而  $\alpha$  是  $X^p - a \in F[X]$  的任意一个根。证明

$$F(\alpha) \neq F(\alpha^p) \iff [F(\alpha) : F] = p.$$

7. 设  $F$  是一个域且  $\text{char } F = p > 0$ . 令  $F_p = \{a^p - a \mid a \in F\}$ . 证明:

(i) 存在  $F$  的一个  $p$  次循环扩域的充要条件是  $F \neq F_p$ ;

(ii) 如果存在  $F$  的一个  $p$  次循环扩域, 那么对于任意  $n \geq 1$ , 都存在  $F$  的  $p^n$  次循环扩域。

8. 设  $p$  是一个素数,  $K$  是域  $F$  上一个  $p$  次可分扩域。证明, 存在  $F$  的一个有限次扩域  $M$ , 使得  $KM$  是  $M$  的一个  $p$  次循环扩域。

### 3.8 关于有限群的若干结果

我们以下将要讨论一个系数在某个域内的代数方程在什么时候可以用“根号解”的问题。在此之前, 需要关于有限群的一些

预备知识.

首先证明关于交错群的一个性质.

一个群  $G$  叫做单群, 如果除开  $G$  本身和单位子群  $\{1\}$  外,  $G$  没有其它的正规子群. 因为一个 Abel 群的子群都是正规的. 所以一个 Abel 群是单的必要且只要它没有异于它本身和  $\{1\}$  的真子群.

显然, 素数阶的循环群是单的 Abel 群. 反过来, 任何一个有限的单 Abel 群  $G \neq \{1\}$  一定是某一素数阶的循环群. 事实上, 设  $a \in G$ ,  $a \neq 1$ , 则  $a$  生成  $G$  的一个循环子群  $\langle a \rangle$ .  $\langle a \rangle \neq \{1\}$  所以必须  $\langle a \rangle = G$ . 如果  $a$  的阶  $n = |G|$  是一个合数. 则  $n = n_1 n_2$ ,  $1 < n_1 < n$ ,  $1 < n_2 < n$ . 于是  $a^{n_1}$  生成  $G$  的一个  $n_2$  阶的真子群, 这与  $G$  的单性矛盾.

最简单的一类非 Abel 单群就是  $n \geq 5$  时, 交错群  $A_n$ . 为了证明  $A_n (n \geq 5)$  是单群, 先证明两个引理.

**引理 3.8.1** 设  $n \geq 3$ . 令  $i, j$  是  $\{1, 2, \dots, n\}$  中不同的元素. 则  $A_n$  由一切 3-轮换  $\{(i, j, k) \mid 1 \leq k \leq n, k \neq i, j\}$  生成.

**证**  $n = 3$  时是显然的. 设  $n > 3$ . 因为  $A_n$  是由一切  $n$  次偶置换组成, 所以  $A_n$  的每一个元素都可以表示成形如

$$(ab)(cd) \text{ 或 } (ab)(ac)$$

的乘积, 这里  $a, b, c, d$  是  $\{1, 2, \dots, n\}$  中互不相同的元素. 然而

$$(ab)(cd) = (acb)(acd),$$

$$(ab)(ac) = (acb).$$

所以  $A_n$  由一切 3-轮换生成. 每一个 3-轮换都具有下列形式之一:

$$(ija), (iaj), (iab), (jab), \text{ 或 } (abc),$$

这里  $a, b, c \neq i$  或  $j$ , 且互不相同. 因为

$$(iaj) = (ija)^2, (iab) = (ijb)(ija)^2,$$

$$(jab) = (ijb)^2(ija), (abc) = (ija)^2(ijc)(ijb)^2(ija),$$

所以  $A_n$  由  $\{(ijk) \mid 1 \leq k \leq n, k \neq i, j\}$  生成. ■

**引理 3.8.2** 设  $n \geq 3$  而  $N$  是  $A_n$  的一个正规子群. 如果  $N$  含有一个 3- 轮换, 则  $N = A_n$ .

**证** 设  $N$  含有一个 3- 轮换  $(ijk)$ . 那么对于任意  $l, 1 \leq l \leq n, l \neq i, j, k$ , 我们有

$$(ijl) = (ij)(kl)(ijk)^2(kl)(ij) \in N.$$

因而  $N$  含有一切  $(ijk), 1 \leq k \leq n, k \neq i, j$ , 由 3.8.1,  $N = A_n$ .

**定理 3.8.3** 当  $n \geq 5$  时,  $A_n$  是单群.

**证** 设  $N$  是  $A_n$  的一个正规子群. 且  $N \neq \{1\}$ , 我们证明,  $N$  一定含有一个 3- 轮换, 从而由 3.8.2,  $N = A_n$ . 我们分别就以下情况来考虑:

1. 如果  $N$  含有一个 3- 轮换, 这时已无须证明.
2.  $N \ni \sigma$ , 而  $\sigma$  被表成不相交的轮换的积时, 至少有一个长度  $r \geq 4$  的轮换. 这时

$$\sigma = (a_1 a_2 \cdots a_r) \tau.$$

令  $\delta = (a_1 a_2 a_3) \in A_n$ . 则

$$N \ni \sigma^{-1} \delta \sigma \delta^{-1} = (a_1 a_3 a_r).$$

3.  $N \ni \sigma$ , 而  $\sigma$  被表成不相交的轮换的积时, 至少有两个因子是 3- 轮换. 这时

$$\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \tau.$$

令  $\delta = (a_1 a_2 a_4) \in A_n$ . 则

$$N \ni \sigma^{-1} \delta \sigma \delta^{-1} = (a_1 a_4 a_2 a_6 a_3).$$

于是由情形 2,  $N$  含有一个 3- 轮换.

4.  $N \ni \sigma$ ,  $\sigma$  是一个 3- 轮换和一些 2- 轮换(不相交)的积. 这时  $\sigma = (a_1 a_2 a_3) \tau$ ,  $\tau$  是一些 2- 轮换的积, 于是

$$N \ni \sigma^2 = (a_1 a_2 a_3)^2 \tau^2 = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2).$$

5. 设  $N$  的每一个元素都是一些不相交的 2- 轮换的积. 设  $\sigma \in N$ . 则

$$\sigma = (a_1 a_2)(a_3 a_4) \tau,$$

这里  $\tau$  是一些不相交的 2- 轮换的积, 且不出现  $a_1, a_2, a_3, a_4$ . 令  $\delta = (a_1 a_2 a_3) \in A_n$ . 则

$$N \ni \sigma^{-1} \delta \sigma \delta^{-1} = (a_1 a_3)(a_2 a_4).$$

因为  $n \geq 5$ , 所以存在  $b \in \{1, 2, \dots, n\}$  且  $b \neq a_1, a_2, a_3, a_4$ , 令  $\alpha = (a_1 a_3 b) \in A_n$ ,  $\beta = (a_1 a_3)(a_2 a_4) \in N$ . 则

$$N \ni \beta^{-1} \alpha \beta \alpha^{-1} = (a_1 a_3 b).$$

以上五种情形穷尽了  $N$  中元素一切可能的形式, 这样,  $A_n$  没有非平凡正规子群, 因而是单群. ■

现在介绍可解群的概念.

设  $G$  是一个群. 一个子群序列

$$(1) \quad G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_s = \{1\},$$

其中每一个  $G_i$  都是  $G_{i-1}$  的正规子群,  $1 \leq i \leq s$ , 叫做  $G$  的一个正规列.

例如,  $S_3 \supset A_3 \supset \{1\}$  是三次对称群  $S_3$  的一个正规列. 而

$$S_4 \supset A_4 \supset V \supset W \supset \{1\},$$

这里  $V = \{1, (12)(34), (13)(24), (14)(23)\}$ ,  $W = \{1, (12)(34)\}$ , 是四次对称群  $S_4$  的一个正规列.

给了  $G$  的一个正规列(1), 相应地就得到一个商群序列

$$(2) \quad G/G_1, G_1/G_2, \dots, G_{s-1}/G_s \cong G_{s-1}.$$

一个群  $G$  叫做一个可解群, 如果  $G$  有一个正规列(1), 而且每一个商群  $G_{i-1}/G_i$  都是 Abel 群, ( $1 \leq i \leq s$ ).

例如, 在上面所给出的  $S_3$  和  $S_4$  的正规列里,  $S_3/A_3$  是 2 阶循环群,  $A_3$  是 3 阶循环群,  $S_4/A_4$  是 2 阶循环群,  $A_4/V$  是 3 阶循环群.  $V/W$  和  $W$  都是 2 阶循环群, 它们都是 Abel 群. 因此  $S_3$  和  $S_4$  都是可解群. 另外, Abel 群自然都是可解群.

我们还要给出可解群的另一个等价的定义. 首先引入导出列的概念.

令  $G$  是一个群. 令  $G^{(1)} = [G, G]$  是  $G$  的换位子群, 即是由  $G$

的一切换位子  $aba^{-1}b^{-1}$  ( $a, b \in G$ ) 所生成的子群.  $G^{(1)}$  是  $G$  的一个正规子群, 因为对于  $a \in G$  和  $b \in G^{(1)}$ , 我们有  $aba^{-1} = aba^{-1}b^{-1}b \in G^{(1)}$ .

设  $n > 1$ . 如果  $G^{(n-1)}$  已被定义, 我们定义  $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ . 这样, 我们就得到  $G$  的一个子群序列

$$(3) \quad G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(n)} \supseteq \cdots.$$

序列(3)叫做  $G$  的导出列.

根据换位子群的定义可知, (3)中每一个商群  $G^{(i-1)}/G^{(i)}$  都是 Abel 群,  $i \geq 1$ .

**定理 3.8.4** 一个群  $G$  是可解的必要且只要存在一个正整数  $n$ , 使得  $G^{(n)} = \{1\}$ .

**证** 如果  $G$  是可解群, 那么  $G$  有一个正规列(1), 其中每一个商群  $G_{i-1}/G_i$  都是 Abel 群 ( $1 \leq i \leq s$ ). 因为  $G/G_1$  是 Abel 群, 所以对于任意  $a, b \in G$ , 我们有  $aba^{-1}b^{-1} \in G_1$ , 所以  $G^{(1)} \subseteq G_1$ . 一般, 由  $G_{i-1}/G_i$  是 Abel 群可以推出  $G^{(i)} \subseteq G_i$ . 取  $n = s$ , 则  $G^{(n)} = \{1\}$ .

反之, 设有某一个  $n > 0$  使得  $G^{(n)} = \{1\}$ . 则

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{1\}$$

是  $G$  的一个正规列, 且  $G^{(i-1)}/G^{(i)}$  是 Abel 群,  $1 \leq i \leq n$ , 所以  $G$  是可解群. ■

**推论 3.8.5** 可解群的任意子群和任意同态像都是可解群.

**证** 设对某一个  $n > 0$ ,  $G^{(n)} = \{1\}$ . 令  $H$  是  $G$  的一个子群. 则  $H^{(i)} \subseteq G^{(i)}$ , 从而  $H^{(n)} = \{1\}$ .

设  $N$  是  $G$  的一个正规子群, 则对任意  $i > 0$ ,

$$(G/N)^{(i)} = NG^{(i)}/N.$$

于是  $(G/N)^{(n)} = N/N = \{1\}$ . ■

**定理 3.8.6** 设  $N$  是群  $G$  的一个正规子群.  $G$  是可解群必要且只要  $N$  和  $G/N$  都是可解群.

证 由 3.8.5, 若  $G$  是可解群, 则  $N$  和  $G/N$  都是可解群.

反之, 由于  $G/N$  可解, 所以  $G/N$  有正规列

$$G/N = G_0/N \supseteq G_1/N \supseteq \cdots \supseteq G_s/N = \{1\},$$

商群  $G_{i-1}/G_i \cong (G_{i-1}/N)/(G_i/N)$  是 Abel 群,  $1 \leq i \leq s$ . 又因为  $N$  可解, 所以  $N$  有正规列

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_t = \{1\}.$$

商群  $N_{j-1}/N_j$  是 Abel 群,  $1 \leq j \leq t$ . 于是

$$G \supseteq G_1 \supseteq \cdots \supseteq G_s = N \supseteq N_1 \supseteq \cdots \supseteq N_t = \{1\}$$

是满足可解群定义的一个正规列. ■

推论 3.8.7 设  $H_1, \dots, H_s$  是群  $G$  的正规子群.

令  $N = \bigcap_{i=1}^s H_i$ . 如果每一个商群  $G/H_i$  ( $1 \leq i \leq s$ ) 都是可解群, 则  $G/N$  也是可解群.

证 对  $s$  作归纳法. 对于任意  $i \neq j$ ,  $1 \leq i, j \leq s$ , 我们有

$$G/H_i \supseteq H_j H_i / H_i \cong H_j / H_i \cap H_j.$$

所以  $H_j / H_i \cap H_j$  与可解群  $G/H_i$  的一个子群同构, 因而是可解群, 另一方面,

$$(G/H_i \cap H_j) / (H_i / H_i \cap H_j) \cong G/H_i$$

也是可解群. 于是由 3.8.6,  $G/H_i \cap H_j$  是可解群.

假设  $s > 2$ , 并且已知  $G / \bigcap_{i=1}^{s-1} H_i$  是可解群. 令  $M = \bigcap_{i=1}^{s-1} H_i$ . 于是

$$G/M \supseteq M H_s / M \cong H_s / M \cap H_s = H_s / N.$$

因此  $H_s$  是可解群. 又因为

$$(G/N) / (H_s/N) \cong G/H_s$$

可解, 所以由 3.8.6,  $G/N$  是可解群. ■

定理 3.8.8 设  $G \neq \{1\}$  是一个有限群.  $G$  是可解的必要且只要存在一个正规列

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{1\},$$



其中每一个商群 $G_{i-1}/G_i$  ( $1 \leq i \leq s$ ) 都是素数阶的循环群.

**证** 设 $G$ 是可解群. 于是 $G$ 有一个正规列

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = \{1\},$$

其中每一个 $G_{i-1}/G_i$  ( $1 \leq i \leq s$ ) 都是 Abel 群. 在商群 $G/G_1$ 中存在一个异于 $G/G_1$ 的最大阶的正规子群 $N_1/G_1$ . 如果 $N_1 \neq G$ , 那么在商群 $N_1/G_1$ 中存在一个异于 $N_1/G_1$ 的最大阶的正规子群 $N_2/G_1$ . 如此继续下去, 最后一定有某一个 $t > 0$ , 使得 $N_t = G_1$ . 这样就得到一个子群序列

$$G = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_t = G_1.$$

$N_{i-1}/N_i$  是单 Abel 群, 所以是一个素数阶循环群,  $1 \leq i \leq t$ . 再对 $G_1/G_2, G_2/G_3, \cdots$  作同样的考虑. 最后我们得到 $G$ 的一个正规列

$$G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = \{1\},$$

其中每一个商群 $N_{i-1}/N_i$  都是素数阶的循环群.

反过来是显然的. ■

最后, 由 3.8.3, 我们立即得到

**定理 3.8.9** 当 $n \geq 5$  时,  $n$  次对称群 $S_n$  不是可解群.

**证** 如果 $S_n$  可解, 则 $A_n$  可解. 然而由 3.8.3, 当 $n \geq 5$  时,  $A_n$  没有非平凡的正规子群, 且 $A_n$  不是 Abel 群, 所以 $A_n$  不可能有满足可解群定义的正规列. ■

### 3.9 可解扩域和根号扩域

设 $F$ 是一个域.  $F$ 的一个 Galois 扩域 $K$ 叫做 $F$ 的一个可解扩域, 如果 $K/F$ 的 Galois 群 $G(K/F)$ 是一个可解群, 这时 $K/F$ 叫做一个可解扩张.

**例 1** Abel 扩张都是可解扩张.

**例 2**  $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$  是 $\mathbb{Q}$ 的一个可解扩域. 因为 $K/\mathbb{Q}$ 是 Galois 扩张, 它的 Galois 群 $G(K/\mathbb{Q})$ 与 $S_3$ 同构, 后者是一个

可解群 (3.2 例 4) .

**定理 3.9.1** 设  $M$  是域  $F$  的一个扩域.  $K$  和  $L$  都是  $M/F$  的中间域. 如果  $K$  和  $L$  都是  $F$  的有限次可解扩域, 那么合成域  $KL$  也是  $F$  的一个有限次可解扩域.

**证** 因为  $K/F$  和  $L/F$  都是有限次 Galois 扩张, 所以由 3.1.9,  $KL/F$  也是有限次 Galois 扩张. 令  $G = G(KL/F)$ ,  $N = G(KL/L)$ . 由 3.3.4,  $N$  是  $G$  的正规子群, 且  $G/N \cong G(L/F)$ . 由题设,  $G/N$  是可解群. 又由 3.1.9,

$$N = G(KL/L) \cong G(K/K \cap L) \subseteq G(K/F).$$

所以  $N$  也是可解群. 于是由 3.8.6,  $G$  是可解群, 从而  $KL$  是  $F$  可解扩域. ■

**定理 3.9.2** 设  $F$  是一个域,  $\Omega$  是  $F$  的一个代数闭包. 令  $F \subseteq K \subseteq L \subseteq \Omega$  是一串扩域, 其中  $K$  是  $F$  的有限次可解扩域而  $L$  是  $K$  的有限次可解扩域. 那么存在  $F$  的一个有限次可解扩域  $M$ , 使得  $F \subseteq K \subseteq L \subseteq M \subseteq \Omega$ .

**证**  $L/K$  和  $K/F$  都是有限次可分扩张, 所以  $L/F$  也是有限次可分扩张. 于是由 3.1.5, 存在  $F$  的一个有限次 Galois 扩域  $P$ , 使得

$$F \subseteq K \subseteq L \subseteq P \subseteq \Omega.$$

令  $G = G(P/F)$ ,  $N = G(P/K)$ ,  $H = G(P/L)$ , 则  $H \triangleleft N$ ,  $N \triangleleft G$ , 我们有

$$N/H \cong G(L/K), \quad G/N \cong G(K/F).$$

所以  $N/H$ ,  $G/N$  都是可解群. 设  $H_1, \dots, H_s$  是  $G$  中一切与  $H$  共轭的子群, 令  $U = \bigcap_{i=1}^s H_i$ . 因为  $N \triangleleft G$ ,  $H \triangleleft N$ , 所以  $H_i \triangleleft N$ , 且  $N/H_i \cong N/H$ , 因此  $N/H_i$  是可解群,  $1 \leq i \leq s$ . 于是由 3.8.7,  $N/U$  是可解群.

令  $M$  是与  $G$  的子群  $U$  相对应的  $P/F$  的中间域. 则

$[M:F] \leq [P:F] < \infty$ .  $U \cong G(P/M)$ .  $U \subseteq H$ , 所以  $M \supseteq L$ .  
 又因为  $U \triangleleft G$ , 所以  $M$  是  $F$  的 Galois 扩域, 且  $G(M/F) \cong G/U$ .  
 这些子群与中间域的对应关系如下:

$$P \longleftrightarrow \{1\}$$

$$M \longleftrightarrow U$$

$$L \longleftrightarrow H$$

$$K \longleftrightarrow N$$

$$F \longleftrightarrow G$$

我们有

$$(G/U)/(N/U) \cong G/N \cong G(K/F).$$

而  $N/U$ ,  $G/N$  都可解, 所以由 3.8.6,  $G/U$  是可解群. 于是  $G(M/F)$  是可解群. 这样一来,  $M$  就是  $F$  的一个满足定理要求的有限次可解扩域. ■

现在我们引入根号扩域的概念.

设  $F$  是一个域.  $F$  的一个扩域  $K$  叫做  $F$  的一个根号扩域, ( $K/F$  称为根号扩张) 如果存在  $K/F$  的一串中间域  $F = F_0, F_1, \dots, F_r = K$ :

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_r = K,$$

使得  $F_i = F_{i-1}(\alpha_i)$ ,  $\alpha_i^{n_i} \in F_{i-1}$ , 其中  $n_i$  是一个不能被  $\text{char } F$  整除的正整数,  $1 \leq i \leq r$ .

由定义立即得出以下简单事实:

1. 域  $F$  的根号扩域一定是有限次扩域.
2. 如果  $K/F$  和  $L/K$  都是根号扩张, 则  $L/F$  也是根号扩张.
3. 设  $K$  是  $F$  的一个根号扩域, 而  $K'$  是  $K$  在  $F$  上一个与  $K$  共轭的域, 则  $K'$  也是  $F$  的根号扩域.
4. 设  $K$  和  $L$  都被包含在  $F$  的一个共同的扩域内. 如果  $K/F$ ,  $L/F$  都是根号扩张, 则  $KL/F$  也是根号扩张.

可解扩张和根号扩张之间的关系由以下定理指出.

**定理 3.9.3** 设  $F$  是一个域,  $\Omega$  是  $F$  的一个代数闭包.

(i) 设  $K(\subseteq \Omega)$  是  $F$  的一个根号扩域. 那么存在  $F$  的一个有限次可解扩域  $L$ , 使得  $F \subseteq K \subseteq L \subseteq \Omega$ .

(ii) 设  $K(\subseteq \Omega)$  是  $F$  的一个有限次可解扩域, 且  $[K:F]$  不能被  $\text{char} F$  整除. 那么存在  $F$  的一个根号扩域  $L$ , 使得  $F \subseteq K \subseteq L \subseteq \Omega$ .

**证** (i) 对域次数  $n=[K:F]$  作归纳法来证明  $L$  的存在.  
 $n=1$  时,  $K=F$ , 这时取  $L=K=F$  即可.

设  $n>1$ . 假定存在  $K/F$  的中间域序列:

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K,$$

$F_i = F_{i-1}(\alpha_i)$ ,  $\alpha_i^{n_i} \in F_{i-1}$ ,  $\text{char} F \nmid n_i$ , 且  $[F_i:F_{i-1}] > 1$  ( $1 \leq i \leq r$ ). 令  $K' = F_{r-1}$ . 则  $K' \neq K$ ,  $K = K'(\alpha)$ ,  $\alpha^m \in K'$  ( $\alpha = \alpha_r$ ,  $m = n_r$ ). 则  $[K':F] < [K:F]$  且  $K'/F$  是根号扩张. 由归纳法的假设, 存在  $F$  的有限次可解扩域  $L'$ , 使得

$$F \subseteq K' \subseteq L' \subseteq \Omega.$$

因为  $\text{char} F \nmid m$ , 所以  $\Omega$  含有一个本原  $m$  次单位根  $\zeta$ . 令  $P = F(\zeta) \subseteq \Omega$ . 由 3.5.2,  $P$  是  $F$  的有限次 Abel 扩域, 又  $L'$  是  $F$  的有限次可解扩域. 于是由 3.9.1,  $M = L'P = L'(\zeta)$  是  $F$  的一个有限次可解扩域.

因为  $\alpha^m \in K' \subseteq L' \subseteq M$ , 且  $\zeta \in P \subseteq M$ . 所以由 3.7.7,  $M(\alpha)$  是  $M$  的一个有限次循环扩域, 因而是  $M$  的一个有限次可解扩域. 在扩域序列  $F \subseteq M \subseteq M(\alpha) \subseteq \Omega$  里,  $M/F$ ,  $M(\alpha)/M$  都是有限次可解扩张, 由 3.9.2, 存在  $F$  的一个有限次可解扩域  $L$ , 使得

$$F \subseteq M \subseteq M(\alpha) \subseteq L \subseteq \Omega.$$

因为  $K = K'(\alpha) \subseteq L'(\alpha) \subseteq M(\alpha)$ , 所以  $F \subseteq K \subseteq L \subseteq \Omega$ .

(ii) 仍是对  $n=[K:F]$ ,  $\text{char} F \nmid n$ , 作数学归纳法来证明  $L$  的存在.

$n=1$  时显然. 这时  $K=F$ .  $L=K=F$ .

设  $n > 1$ , 且  $\text{char} F \nmid n$ . 令  $G = G(K/F)$ . 则  $G$  是有限可解群. 于是由 3.8.8, 存在  $G$  的一个正规列

$$G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}.$$

其中每一个商群  $N_{i-1}/N_i$  都是阶为某一素数  $q_i$  的循环群,  $1 \leq i \leq r$ . 因为  $\text{char} F \nmid n$ , 而  $q_i | n$ , 所以  $\text{char} F \nmid q_i$  ( $1 \leq i \leq r$ ).

记  $N = N_1$ ,  $N \triangleleft G$ , 商群  $G/N$  是素数  $q = q_1$  阶的循环群. 令  $K'$  是  $K/F$  中与  $N$  对应的中间域. 则  $G(K/K') = N$ ,  $G(K'/F) \cong G/N$ , 所以  $K'$  是  $F$  的  $q$  次循环扩域.

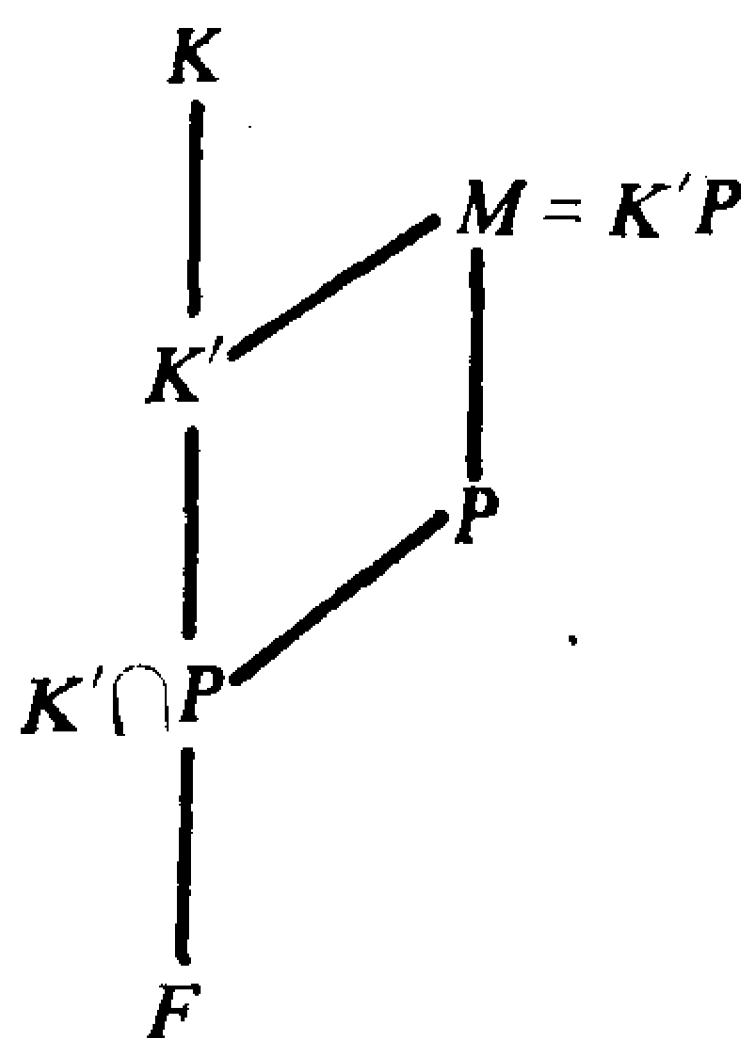
因为  $\text{char} F \nmid q$ , 所以  $\Omega$  含有一个本原  $q$  次单位根  $\eta$ . 令  $P = F(\eta)$ ,  $M = K'P = K'(\eta)$ . 因为  $K'/F$  是有限次 Galois 扩张, 所以由 3.1.9,  $M = K'P$  是  $P$  的 Galois 扩域, 且

$$G(M/P) \cong G(K'/K' \cap P) \subseteq G(K'/F) \cong G/N.$$

因为  $G/N$  是素数  $q$  阶的循环群, 所以  $|G(M/P)| = q$  或  $1$ .

如果  $|G(M/P)| = q$ , 则  $G(M/P)$  是  $q$  阶循环群. 于是  $M$  是  $P$  的  $q$  次循环扩域, 而  $\eta \in P$ , 所以由 3.7.6 和 3.7.7, 存在  $\alpha \in M$ , 使得  $\alpha^q \in P$ .

如果  $|G(M/P)| = 1$ , 则  $M = P$ .



不论哪一个情形,  $M$  都是  $P$  的根号扩域. 又  $P = F(\eta)$  是  $F$  的根号扩域. 所以  $M$  是  $F$  的根号扩域.

因为  $K/F$  是有限次 Galois 扩张, 所以由 3.1.9,  $KM/M$  也是 Galois 扩张, 并且

$$G(KM/M) \cong G(K/K \cap M)$$

$$\subseteq G(K/F).$$

由于  $G(K/F)$  是有限可解群, 所以  $G(KM/M)$  也是有限可解群, 从而  $KM$  是  $M$  的有限次可解扩域, 因为  $M = K'P$ , 所以  $K' \subseteq K \cap M$ .



对于  $f(X)$  的系数施行有限次加、减、乘、除及开方运算所组成的公式，使得这个方程的每一个根都可以由这个公式表示出来？

假设这样一个公式存在。由于加、减、乘、除运算可以在基础域里进行，而对一个数  $a$  开  $n$  次方相当于求一个数  $\alpha$ ，使得  $\alpha^n = a$ ，因此，存在一串扩域

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K,$$

其中  $F_i = F_{i-1}(\alpha_i)$ ,  $\alpha_i^{n_i} \in F_{i-1}$  ( $1 \leq i \leq r$ )，使得  $f(X)$  的每一个根都在  $K$  内。这相当于说，存在  $F$  的一个根号扩域  $K$ ，使得  $f(X)$  的每一个根都包含在  $K$  内。

反过来，设  $f(X)$  是数域  $F$  上一个多项式。如果存在  $F$  的一个根号扩域  $K$ ，使得  $f(X)$  的每一个根都包含在  $K$  内，那么一定存在方程  $f(X) = 0$  的根的表达式，这个表达式是由  $f(X)$  的系数经过有限次加、减、乘、除及开方运算组成的。

一般，设  $F$  是任意一个域。 $f(X) \in F[X]$ 。方程  $f(X) = 0$  说是在  $F$  上可以用根号解，如果存在  $F$  的一个根号扩域  $K$ ，使得  $f(X)$  的全部根都在  $K$  内。

由前一节的结果。很容易得出域  $F$  上一个方程在  $F$  上可以用根号解的充要条件。首先注意一个简单的事实。

**引理 3.10.1** 设  $F$  是一个域， $f(X)$  是  $F[X]$  中一个次数大于零的多项式， $L$  是  $f(X)$  在  $F$  上一个分裂域。如果  $\text{char} F$  不能整除  $[L : F]$ ，则  $L$  是  $F$  的一个 Galois 扩域。

**证** 只要证明  $L/F$  是可分扩张。当  $\text{char} F = 0$  时显然。设  $\text{char} F = p > 0$ 。令  $\alpha$  是  $L$  的任意元素。则  $[F(\alpha) : F] \mid [L : F]$ 。因为  $p \nmid [L : F]$ ，所以  $p \nmid [F(\alpha) : F]$ 。所以  $F(\alpha)$  是  $F$  的可分扩域，因而  $\alpha$  是  $F$  上可分元素。所以  $L$  是  $F$  上可分扩域。 ■

**定理 3.10.2** 设  $F$  是一个域， $f(X) \in F[X]$  是一个次数大于零的多项式， $L$  是  $f(X)$  在  $F$  上一个分裂域，且  $\text{char} F \nmid [L : F]$ 。那么方程  $f(X) = 0$  在  $F$  上可以用根号解必要且只要  $L$  是  $F$  的一

个有限次可解扩域。

证 设  $f(X)=0$  在  $F$  上可以用根号解。于是存在  $F$  的一个根号扩域  $K$ , 使得  $F \subseteq L \subseteq K$ 。由 3.9.3, 存在  $F$  的一个有限次可解扩域  $M$ , 使得  $F \subseteq K \subseteq M$ 。从而有  $F \subseteq L \subseteq M$ 。

因为  $M/F$  是有限次可解扩张, 又由 3.10.1,  $L/F$  是 Galois 扩张, 所以  $G(M/F)$  是可解群, 且  $G(M/L) \triangleleft G(M/F)$ 。于是

$$G(L/F) \cong G(M/F)/G(M/L)$$

是可解群, 因而  $L$  是  $F$  的有限次可解扩域。

反之, 设  $L = F(\alpha_1, \dots, \alpha_m)$  是多项式  $f(X)$  在  $F$  上的分裂域。由题设,  $L/F$  是有限次可解扩张, 且  $\text{char } F \nmid [L:F]$ 。由 3.9.3, 存在  $F$  的一个根号扩域  $K$ , 使得  $F \subseteq L \subseteq K$ 。所以  $f(X)=0$  的全部根都包含在  $F$  的一个根号扩域内, 因而  $f(X)=0$  可以用根号解。 ■

设  $F$  是一个域,  $f(X) \in F[X]$  是  $F$  上一个可分多项式。令  $L$  是  $f(X)$  在  $F$  上一个分裂域。  $L$  自然是  $F$  的 Galois 扩域。 Galois 群  $G(L/F)$  叫做多项式  $f(X)$  的 (或方程  $f(X)=0$  的) Galois 群。

这个定义不依赖于分裂域  $L$  的选取。事实上, 设  $L$  和  $L'$  都是  $f(X)$  在  $F$  上分裂域。那么  $L$  与  $L'$  是  $F$ -同构的。所以  $G(L/F) \cong G(L'/F)$ 。因此, 多项式  $f(X) \in F[X]$  的 Galois 群除同构外是唯一确定的。

如同定理 3.10.2 的证明一样, 我们得到以下

**定理 3.10.3** 设  $f(X)$  是域  $F$  上一个可分多项式。

(i) 如果方程  $f(X)=0$  在  $F$  上可以用根号解, 则方程  $f(X)=0$  的 Galois 群  $G$  是一个可解群。

(ii) 如果方程  $f(X)=0$  的 Galois 群  $G$  是可解群, 并且  $\text{char } F$  不能整除  $G$  的阶, 则方程  $f(X)=0$  在  $F$  上可以用根号解。 ■



推论 3.10.4 设  $F$  是一个特征为 0 的域.  $f(X)$  是  $F$  上一个多项式, 方程  $f(X)=0$  在  $F$  上可以用根号解必要且只要方程  $f(X)=0$  的 Galois 群是可解群. ■

## 习 题

1. 设  $F$  是一个域,  $\text{char} F \neq 2$ ,  $f(X) \in F[X]$  是一个最高次项系数为 1 的  $n(>0)$  次可分多项式,  $\alpha_1, \dots, \alpha_n$  是  $f(X)$  在  $F$  的某一个扩域内的全部根,  $K = F(\alpha_1, \dots, \alpha_n)$ . 令

$$d = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

$G$  是  $f(X)$  的 Galois 群. 将  $G$  看作  $S_n$  的一个子群. 证明, 在 Galois 基本定理中与子群  $G \cap A_n$  对应的中间域是  $F(d)$ .

2. 在前题的假设和记号下, 令

$$D = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

证明,  $G \subset A_n$  必要且只要  $D$  是  $F$  中某个元素的平方 ( $D$  称为  $f(X)$  的判别式).

## 3.11 $n$ 次一般方程

我们将证明, 当  $n > 4$  时, 特征为 0 的域上  $n$  次一般方程不能用根号解.

先证明一个引理.

引理 3.11.1 设  $k$  是一个域,  $K = k(x_1, \dots, x_n)$  是  $k$  上  $n$  个不相关不定元  $x_1, \dots, x_n$  的有理分式域. 令

$$\begin{aligned} a_1 &= \sum_{i=1}^n x_i, \quad a_2 = \sum_{1 \leq i < j \leq n} x_i x_j, \dots, \\ a_s &= \sum_{1 \leq i_1 < \dots < i_s \leq n} x_{i_1} \dots x_{i_s}, \dots, \quad a_n = x_1 \dots x_n \end{aligned}$$

是  $x_1, \dots, x_n$  的初等对称多项式;  $F = k(a_1, \dots, a_n)$ . 则  $K$  是  $F$  的

Galois 扩域, 并且 Galois 群  $G(K/F)$  与  $n$  次对称群  $S_n$  同构.

证  $\{1, 2, \dots, n\}$  的每一个置换  $\sigma$  唯一地确定  $K$  的一个  $k$ -自同构, 仍以  $\sigma$  表示, 使得

$$\sigma(x_i) = x_{\sigma(i)}, \quad i = 1, 2, \dots, n.$$

并且不同的置换所确定的自同构也不相同. 令  $G$  是如上所给出的  $K$  的  $k$ -自同构的全体. 那么  $G$  是  $K$  的一切  $k$ -自同构所成的群  $G(K/k)$  的一个子群, 且  $G \cong S_n$ . 令

$$F_0 = K^G = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

是  $G$  的固定域. 那么  $k \subseteq F \subseteq F_0 \subseteq K$ . 由 3.3.2,  $K/F_0$  是 Galois 扩张. 它的 Galois 群就是  $G$ . 所以  $[K : F_0] = |G| = n!$ . 令

$$\begin{aligned} f(X) &= \prod_{i=1}^n (X - x_i) = X^n - a_1 X^{n-1} + \\ &\quad + a_2 X^{n-2} - \dots + (-1)^n a_n. \end{aligned}$$

则  $f(X) \in F[X]$ .

我们有扩域序列

$$F \subseteq F(x_1) \subseteq F(x_1, x_2) \subseteq \dots \subseteq F(x_1, \dots, x_n) = K.$$

因为  $x_1$  是  $f(X)$  的一个根, 所以  $[F(x_1) : F] \leq \deg f = n$ . 其次,  $x_2$  是多项式  $f(X)/(X - x_1) \in F_1[X]$  的一个根, 这里  $F_1 = F(x_1)$ , 所以

$$[F(x_1, x_2) : F(x_1)] \leq \deg \frac{f(X)}{X - x_1} = n - 1.$$

一般, 对于  $1 \leq s \leq n$ , 我们有

$$[F(x_1, \dots, x_s) : F(x_1, \dots, x_{s-1})] \leq n - s + 1,$$

所以  $[K : F] \leq n!$ .

另一方面, 因为  $F \subseteq F_0 \subseteq K$ , 而  $[K : F_0] = n!$ , 所以  $[K : F] \geq n!$ . 这样一来, 我们有  $[K : F] = n!$ ,  $F = F_0$ , 因此  $K/F$  是 Galois 扩张, 它的 Galois 群与  $S_n$  同构. ■

现在设  $k$  是一个域,  $t_1, \dots, t_n$  是  $k$  上  $n$  个不相关不定元. 令

$F = k(t_1, \dots, t_n)$ . 多项式

$$f(X) = X^n - t_1 X^{n-1} + t_2 X^{n-2} - \dots + (-1)^n t_n \in F[X]$$

叫做  $k$  上  $n$  次一般多项式; 相应地, 方程  $f(X) = 0$  叫做  $k$  上  $n$  次一般方程.

**定理 3.11.2** 设  $k$  是一个域.  $k$  上  $n$  次一般多项式

$$f(X) = X^n - t_1 X^{n-1} + t_2 X^{n-2} - \dots + (-1)^n t_n$$

是  $F$  上一个可分的不可约多项式.  $f(X)$  在  $F$  上的 Galois 群与  $n$  次对称群  $S_n$  同构.

证 令  $\alpha_1, \dots, \alpha_n$  是  $f(X)$  在  $F$  的某一个代数闭包内的全部根,  $K = F(\alpha_1, \dots, \alpha_n)$  是  $f(X)$  在  $F$  上的分裂域. 在  $K[X]$  内, 我们有

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n).$$

由根与系数的关系. 我们有

$$\begin{aligned} t_1 &= \sum_{i=1}^n \alpha_i, & t_2 &= \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j, \dots, \\ t_s &= \sum_{1 \leq i_1 < \dots < i_s \leq n} \alpha_{i_1} \cdots \alpha_{i_s}, \dots, & t_n &= \alpha_1 \cdots \alpha_n. \end{aligned}$$

而  $K = F(\alpha_1, \dots, \alpha_n) = k(t_1, \dots, t_n, \alpha_1, \dots, \alpha_n) = k(\alpha_1, \dots, \alpha_n)$ .

令  $\bar{K} = k(x_1, \dots, x_n)$  是  $k$  上  $n$  个不相关不定元  $x_1, \dots, x_n$  的有理分式域. 设

$$\begin{aligned} f(X) &= \prod_{i=1}^n (X - x_i) = X^n - a_1 X^{n-1} + \\ &\quad + a_2 X^{n-2} - \dots + (-1)^n a_n, \end{aligned}$$

这里

$$a_1 = \sum_{i=1}^n x_i, a_2 = \sum_{1 \leq i < j \leq n} x_i x_j, \dots, a_n = x_1 \cdots x_n,$$

令  $\bar{F} = k(a_1, \dots, a_n) \subseteq \bar{K}$ . 由 3.11.1,  $\bar{K}/\bar{F}$  是  $n!$  次的 Galois 扩张, 且  $G(\bar{K}/\bar{F}) \cong S_n$ .

我们证明, 存在  $K$  到  $\bar{K}$  的  $k$ -同构  $\varphi: K \rightarrow \bar{K}$ , 使得  $\varphi(\alpha_i) = x_i$ ,

$1 \leq i \leq n$ , 如果这个断言被证明, 那么就有  $\varphi(t_i) = a_i$ ,  $1 \leq i \leq n$ , 而  $\varphi(F) = \bar{F}$ . 于是  $K/F$  是 Galois 扩张, 并且  $G(K/F) \cong S_n$ . 从而也就证明了  $f(X)$  在  $F$  上的 Galois 群与  $S_n$  同构, 并且  $f(X)$  是  $F$  上一个可分的不可约多项式.

令  $R = k[t_1, \dots, t_n]$ ,  $\bar{R} = k[a_1, \dots, a_n] \subseteq k[x_1, \dots, x_n]$ . 因为  $t_1, \dots, t_n$  是  $K$  上不相关不定元, 所以映射  $\varphi: t_i \mapsto a_i$  ( $1 \leq i \leq n$ ) 可以自然地开拓为环  $R$  到环  $\bar{R}$  的满同态  $\varphi: R \rightarrow \bar{R}$ . 设

$$h(t_1, \dots, t_n) \in \text{Ker } \varphi.$$

则

$$h(a_1, \dots, a_n) = 0.$$

于是  $k[x_1, \dots, x_n]$  的元素

$$h(a_1(x_1, \dots, x_n), \dots, a_n(x_1, \dots, x_n)) = 0,$$

这里

$$a_s(x_1, \dots, x_n) = \sum_{1 \leq i_1 < \dots < i_s \leq n} x_{i_1} \dots x_{i_s} \quad (1 \leq s \leq n).$$

另一方面,  $\psi: k[x_1, \dots, x_n] \rightarrow k[\alpha_1, \dots, \alpha_n]$ ,  $\psi(x_i) = \alpha_i$  ( $1 \leq i \leq n$ ), 是环同态满射, 而

$$\psi(a_s) = \psi(a_s(x_1, \dots, x_n)) = a_s(\alpha_1, \dots, \alpha_n) = t_s \quad (1 \leq s \leq n),$$

所以  $h(a_1, \dots, a_n) = 0$ , 于是

$$h(t_1, \dots, t_n) = \psi(h(a_1, \dots, a_n)) = 0,$$

从而  $\text{Ker } \varphi = 0$ . 这样  $\varphi: R \rightarrow \bar{R}$  是环同构映射.

$\varphi$  可以唯一地开拓为  $R$  的商域  $F = k(t_1, \dots, t_n)$  到  $\bar{R}$  的商域  $\bar{F} = k(a_1, \dots, a_n)$  上的同构映射, 因而可以唯一地开拓为多项式环  $F[X]$  到多项式环  $\bar{F}[X]$  上的同构映射  $\varphi: F[X] \rightarrow \bar{F}[X]$ . 我们有

$$\varphi(f(X)) = \bar{f}(X).$$

于是  $\varphi$  又可以开拓为  $f(X)$  在  $F$  上的分裂域  $K$  到  $\bar{f}(X)$  在  $\bar{F}$  上的分裂域  $\bar{K}$  上的同构映射. 在这个开拓下,  $\varphi(\alpha_i) = x_i$  ( $1 \leq i \leq n$ ). 定理被证明. ■

由这个定理，我们立即得到以下

**定理 3.11.3** 设  $k$  是一个特征为 0 的域， $t_1, \dots, t_n$  是  $k$  上不相关不定元， $F = k(t_1, \dots, t_n)$ 。  $n$  次一般方程

$$f(X) = X^n - t_1 X^{n-1} + t_2 X^{n-2} - \dots + (-1)^n t_n = 0$$

在  $F$  上可以用根号解的必要且充分条件是  $n \leq 4$ 。

**证**  $f(X) = 0$  在  $F$  上可以用根号解  $\iff f(X)$  的 Galois 群是可解群  $\iff n$  次对称群  $S_n$  是可解群  $\iff n \leq 4$ 。 ■

由 3.11.2，我们还得到以下

**定理 3.11.4** 给定一个有限群  $G$  和一个素数  $p$  或 0，那么存在一个特征为  $p$  或 0 的域  $E$  和  $E$  的一个 Galois 扩域  $K$ ，使得  $G(K/E) \cong G$ 。

**证** 设  $G$  的阶为  $n$ ，那么由 Cayley 定理， $G$  与  $n$  次对称群  $S_n$  的一个子群  $H$  同构。令  $k$  是一个域， $\text{char } k = p$  或 0， $t_1, \dots, t_n$  是  $k$  上  $n$  个不相关不定元。令  $F = k(t_1, \dots, t_n)$ 。取  $K$  是多项式

$$f(X) = X^n - t_1 X^{n-1} + t_2 X^{n-2} - \dots + (-1)^n t_n \in F[X]$$

在  $F$  上的分裂域。则  $K$  是  $F$  的 Galois 扩域，它的 Galois 群  $G(K/F)$  与  $S_n$  同构。对于  $S_n$  的子群  $H$ ，有  $G(K/F)$  的一个与  $H$  同构的子群与它对应，仍记作  $H$ 。令  $E$  是与  $H$  对应的  $K/F$  的中间域，则  $K/E$  是 Galois 扩张，且  $G(K/E) = H \cong G$ 。 ■

**注意** 一般，给定一个域  $F$  和一个有限群  $G$ ，是否存在  $F$  的一个 Galois 扩域  $K$ ，使得  $K/F$  的 Galois 群  $G(K/F) \cong G$ 。这个问题的答案是否定的。只要看一看有限域  $F_q$  或看实数域  $R$  或复数域  $C$  的情形就足以证明这一点。当  $F = Q$  是有理数域时，除了个别的群  $G$  外，这个问题的一般解决也远没有得到。

最后我们讨论一下素数次方程。

**引理 3.11.4** 设  $p$  是一个素数， $f(X)$  是某一个域  $F$  上  $p$  次可分多项式。如果  $f(X)$  的 Galois 群  $G$  不等于  $S_p$ ，则  $f(X)$  在  $F$  上的分裂域可以由  $f(X)$  的任意  $p-2$  个根生成。

证 设  $\alpha_1, \dots, \alpha_p$  是  $f(X)$  在  $F$  的一个代数闭包内的全部根。  
 $K = F(\alpha_1, \dots, \alpha_p)$  是  $f(X)$  在  $F$  上的分裂域。如果  $f(X)$  的某  $p-2$  个根不能生成  $K$ , 那么对  $f(X)$  的根适当编号, 可以假定  $E = F(\alpha_3, \dots, \alpha_p) \subsetneq K$ .  $E$  所对应的  $G$  的子群  $H \neq \{1\}$ . 对于  $\sigma \in G$  来说,  $\sigma \in H \iff \sigma(\alpha_j) = \alpha_j, j=3, \dots, p$ . 所以对换  $(12) \in H \subseteq G$ . 另一方面, 因为  $f(X)$  在  $F$  上不可约, 所以  $[F(\alpha_1) : F] = \deg f = p$ ,  $F \subseteq F(\alpha_1) \subseteq K$ ,  $G$  中与  $F(\alpha_1)$  对应的子群的指数为  $p$ , 所以  $p \mid |G|$ . 因为  $p$  是一个素数, 所以  $G$  含有一个  $p$  阶元素  $\sigma$ . 作为  $\{1, 2, \dots, p\}$  的一个置换,  $\sigma$  是一个  $p$ -轮换. 这样,  $\sigma = (1i_2 \dots i_p)$ , 因此  $\sigma$  的若干次幂必有形状  $\sigma^k = (1j_3 \dots j_p)$ , 其中  $\{j_3, \dots, j_p\} = \{3, \dots, p\}$ . 重新对  $\alpha_3, \dots, \alpha_p$  编号 (这不影响  $E$ ), 可设  $\sigma^k = (12 \dots p) \in G$ , 又  $G \ni (12)$ , 于是  $G = S_p$ . ■

**定理 3.11.5** 设  $F$  是实数域  $R$  的一个子域,  $p$  是一个素数. 如果  $F$  上  $p$  次不可约多项式  $f(X)$  恰有  $p-2$  个实根, 则  $f(X)$  在  $F$  上的 Galois 群等于  $S_p$ .

证 设  $\alpha_1, \dots, \alpha_{p-2}, \alpha_{p-1}, \alpha_p \in \mathbb{C}$  是  $f(X)$  的全部根, 其中  $\alpha_1, \dots, \alpha_{p-2}$  是实根而  $\alpha_{p-1}, \alpha_p$  是一对非实的共轭复根. 那么  $f(X)$  在  $F$  上的分裂域  $K = F(\alpha_1, \dots, \alpha_p)$  不是实数域的子域. 另一方面,  $p-2$  个实根  $\alpha_1, \dots, \alpha_{p-2}$  生成的子域  $E = F(\alpha_1, \dots, \alpha_{p-2})$  是实数域  $R$  的子域, 因此  $E \subsetneq K$ . 于是由 3.11.4,  $f(X)$  在  $F$  上的 Galois 群等于  $S_p$ . ■

**例** 设  $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ . 由 Eisenstein 判定法,  $f(X)$  在  $\mathbb{Q}$  上不可约. 由方程论的知识可知  $f(X)$  恰有三个实根. 所以  $f(X)$  的 Galois 群是  $S_5$ , 因而方程  $X^5 - 4X + 2 = 0$  在  $\mathbb{Q}$  上不能用根号解.

应该指出的是, 一个代数方程能否用根号解是和基础域有关的. 例如, 方程  $X^5 - 4X + 2 = 0$  在有理数域  $\mathbb{Q}$  上不能用根号解, 然而在实数域  $R$  上可以用根号解. 事实上,  $R[X]$  中每一个代数

方程在  $R$  上都可以用根号解, 因为  $C = R(\sqrt{-1})$  就是  $R$  的一个根号扩域.

## 习 题

1. 令  $E$  是  $C$  的扩域,  $E = C(t, u)$ , 其中  $t$  是  $C$  上不定元,  $u$  满足  $C(t)$  上方程  $x^2 + t^2 = 1$ , 确定  $C(t, u)$  在  $C(t^{2m}, u^{2m})$  上的 Galois 群. 其中  $m$  是正整数.

### 3.12 二次、三次和四次方程

设  $k$  是一个特征为 0 的域. 我们给出  $k$  上二次、三次和四次一般方程的解.

**二次方程的解**  $k$  上二次方程有形状

$$(1) \quad x^2 - t_1 x + t_2 = 0.$$

令  $\alpha_1, \alpha_2$  是方程(1)在  $F = k(t_1, t_2)$  的一个代数闭包内的根, 方程(1)的 Galois 群  $S_2$  由恒等置换及对换  $(\alpha_1, \alpha_2)$  构成, 所以  $(\alpha_1 - \alpha_2)^2$  在  $S_2$  的作用下保持不动, 因而  $(\alpha_1 - \alpha_2)^2 \in F$ . 我们有

$$(\alpha_2 - \alpha_1)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = t_1^2 - 4t_2.$$

于是  $\alpha_1 - \alpha_2 = \pm\sqrt{t_1^2 - 4t_2}$ . 又  $\alpha_1 + \alpha_2 = t_1$ . 所以(1)的根的公式是

$$\alpha_1, \alpha_2 = (t_1 \pm \sqrt{t_1^2 - 4t_2})/2.$$

**三次方程的解**  $k$  上三次一般方程有形状

$$(2) \quad x^3 - t_1 x^2 + t_2 x - t_3 = 0.$$

通过未知量的代换

$$X = Y + \frac{1}{3}t_1,$$

方程(2)化为

$$(3) \quad Y^3 + pY + q = 0,$$

$p, q \in F = k(t_1, t_2, t_3)$ . 解(2)只需解(3). 设  $\alpha_1, \alpha_2, \alpha_3$  是方程(3)在  $F$  的某一个代数闭包内的全部根. 对称群  $S_3$  有合成列

$$S_3 \triangleright A_3 \triangleright (1).$$

先在基础域  $k$  内添加一个本原三次单位根  $\zeta$ ,  $\zeta \neq 1$ ,  $\zeta^3 = 1$ . 令

$$\beta = \alpha_1 + \zeta \alpha_2 + \zeta^2 \alpha_3,$$

$$\gamma = \alpha_1 + \zeta^2 \alpha_2 + \zeta \alpha_3.$$

交错群  $A_3$  由 3-轮换  $(\alpha_1, \alpha_2, \alpha_3)$  生成, 所以使  $\beta^3, \gamma^3$  固定. 另一方面,  $S_3$  的任意对换都对调  $\beta^3, \gamma^3$ . 所以  $\beta^3 + \gamma^3, \beta^3 \gamma^3$  在  $S_3$  的每一元素作用下保持不动, 因而属于  $F$ . 我们有

$$\alpha_1 + \alpha_2 + \alpha_3 = 0,$$

$$\alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \alpha_3 \alpha_1 = p,$$

$$\alpha_1 \alpha_2 \alpha_3 = -q.$$

由此得

$$\beta^3 + \gamma^3 = -27q$$

$$\beta^3 \gamma^3 = -27p^3.$$

所以  $\beta^3, \gamma^3$  是二次多项式

$$(4) \quad T^2 + 27qT - 27p^3$$

的根. 多项式(4)称为方程(3)的予解式. 由方程组

$$\alpha_1 + \zeta \alpha_2 + \zeta^2 \alpha_3 = \beta,$$

$$\alpha_1 + \zeta^2 \alpha_2 + \zeta \alpha_3 = \gamma.$$

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

解出

$$\alpha_1 = \frac{1}{3}(\beta + \gamma),$$

$$\alpha_2 = \frac{1}{3}(\zeta \beta + \zeta^2 \gamma),$$



$$\alpha_3 = \frac{1}{3}(\xi^2 \beta + \xi \gamma).$$

通过简单的计算, 我们有

$$\beta = \sqrt[3]{-27q/2 + (3\sqrt{3}/2)\sqrt{4p^3 + 27q^2}},$$

$$\gamma = \sqrt[3]{-27q/2 - (3\sqrt{3}/2)\sqrt{4p^3 + 27q^2}}.$$

**四次方程的解**  $k$  上四次方程

$$x^4 - t_1 x^3 + t_2 x^2 - t_3 x + t_4 = 0$$

通过未知量的代换

$$X = Y + \frac{1}{4}t_1$$

可化为以下形式:

$$(5) \quad Y^4 + pY^2 + qY + r = 0.$$

设  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  是方程(5)在域  $F = k(p, q, r)$  的某一个代数闭包内的根, 对称群  $S_4$  有合成列

$$S_4 \triangleright A_4 \triangleright V \triangleright \{1, (\alpha_1 \alpha_2)(\alpha_3 \alpha_4)\} \triangleright (1),$$

这里  $V = \{1, (\alpha_1 \alpha_2)(\alpha_3 \alpha_4), (\alpha_1 \alpha_3)(\alpha_2 \alpha_4), (\alpha_1 \alpha_4)(\alpha_2 \alpha_3)\}$ . 令

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),$$

$$(6) \quad \beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$

$$\beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

则集  $\{\beta_1, \beta_2, \beta_3\}$  在  $S_4$  的所有置换之下不变. 所以  $\beta_1, \beta_2, \beta_3$  的初等对称多项式属于  $F$ . 我们有

$$\beta_1 + \beta_2 + \beta_3 = 2p,$$

$$\beta_1 \beta_2 + \beta_2 \beta_3 + \beta_3 \beta_1 = p^2 - 4r,$$

$$\beta_1 \beta_2 \beta_3 = -q^2.$$

$\beta_1 \beta_2 \beta_3$  是  $F$  上三次多项式

$$T^3 - 2pT^2 + (p^2 - 4r)T + q^2$$

的根, 这个三次多项式称为方程(5)的三次予解式. 因为  $\alpha_1 + \alpha_2$

$+\alpha_3+\alpha_4=0$ 。所以由(6)，我们有

$$(\alpha_1+\alpha_2)^2=-\beta_1,$$

$$(\alpha_1+\alpha_3)^2=-\beta_2,$$

$$(\alpha_1+\alpha_4)^2=-\beta_3.$$

于是

$$2\alpha_1=\sqrt{-\beta_1}+\sqrt{-\beta_2}+\sqrt{-\beta_3},$$

$$2\alpha_2=\sqrt{-\beta_1}-\sqrt{-\beta_2}-\sqrt{-\beta_3},$$

$$2\alpha_3=\sqrt{-\beta_1}+\sqrt{-\beta_2}-\sqrt{-\beta_3},$$

$$2\alpha_4=-\sqrt{-\beta_1}-\sqrt{-\beta_2}+\sqrt{-\beta_3},$$

并且满足条件

$$\sqrt{-\beta_1}\sqrt{-\beta_2}\sqrt{-\beta_3}=-q.$$

## 第四章 超越扩张

在前面两章里,我们主要讨论了域的代数扩张.在这一章里,我们将一般地研究超越扩张(非代数扩张).

### 4.1 超越基 超越次数

设  $R$  是一个有单位元  $1$  的交换环,  $S$  是  $R$  的一个子环,并且  $S$  含有  $R$  的单位元,对于  $a_1, \dots, a_n \in R$ , 令  $S[a_1, \dots, a_n]$  表示  $a_1, \dots, a_n$  在  $S$  上所生成的  $R$  的子环.

$S$  上  $n$  个不定元多项式环  $S[X_1, \dots, X_n]$  到  $S[a_1, \dots, a_n]$  的映射

$$\begin{aligned}\varphi: S[X_1, \dots, X_n] \ni f(X_1, \dots, X_n) = \\ \sum c_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n} \longmapsto f(a_1, \dots, a_n) = \\ \sum c_{i_1, \dots, i_n} a_1^{i_1} \cdots a_n^{i_n} \in S[a_1, \dots, a_n],\end{aligned}$$

$c_{i_1, \dots, i_n} \in S$ , 是  $S[X_1, \dots, X_n]$  到  $S[a_1, \dots, a_n]$  的同态满射.

如果同态映射  $\varphi$  是单的, 即  $S[X_1, \dots, X_n] \cong S[a_1, \dots, a_n]$ , 那么就说,  $a_1, \dots, a_n$  在  $S$  上代数无关; 如果  $a_1, \dots, a_n \in R$  不是在  $S$  上代数无关的, 那么就说,  $a_1, \dots, a_n$  在  $S$  上代数相关.

根据这个定义, 对于  $R$  的元素  $a_1, \dots, a_n$  和  $R$  的子环  $S$  来说,

$a_1, \dots, a_n$  在  $S$  上代数无关

$\iff \forall f \in S[X_1, \dots, X_n]$ , 若  $f(a_1, \dots, a_n) = 0$  则  $f = 0$ .

$\iff S[a_1, \dots, a_n]$  中一切单项式  $a_1^{i_1} \cdots a_n^{i_n}$  ( $i_1, \dots, i_n$  是任意非负整数) 的集在  $S$  上线性无关.

$R$  的元素  $a$  叫做子环  $S$  上一个超越元, 如果  $a$  在  $S$  上代数无关; 在相反的情形, 就称  $a$  是  $S$  上一个代数元.

设  $A$  是环  $R$  的一个非空子集. 如果  $A$  中任意有限元素都在  $S$

上代数无关, 那么就说  $A$  在  $S$  上代数无关. 空集 ( $\emptyset \subseteq R$ ) 被认为在  $S$  上代数无关.

由以上定义可以直接得出以下结论:

1. 环  $S$  上一个代数无关集的任意子集也在  $S$  上代数无关.
2.  $S$  上代数无关集里的任意元素都是  $S$  上超越元.
3. 设  $S'$  也是环  $R$  的子环且  $S \subseteq S'$ . 如果  $R$  的子集  $A$  在  $S'$  上代数无关, 那么  $A$  也在  $S$  上代数无关.

我们将引入域的超越基的概念, 首先证明一个引理.

**引理 4.1.1** 设  $F$  是一个域,  $K$  是  $F$  的一个扩域,  $A$  和  $B$  是  $K$  的两个子集. 对于  $A$  和  $B$  来说, 以下三个条件是等价的:

- (i)  $A \cap B = \emptyset$  且  $A \cup B$  在  $F$  上代数无关;
- (ii)  $A$  在  $F$  上代数无关而  $B$  在  $F(A)$  上代数无关;
- (iii)  $B$  在  $F$  上代数无关而  $A$  在  $F(B)$  上代数无关.

**证** 由于  $A$  与  $B$  的地位对称性, 我们只需证 (i)  $\iff$  (ii).

(i)  $\implies$  (ii)  $A \subseteq A \cup B$  而  $A \cup B$  在  $F$  上代数无关, 所以  $A$  在  $F$  上代数无关. 我们证明  $B$  在  $F(A)$  上代数无关.

令  $\eta_1, \dots, \eta_m$  是  $B$  中任意有限个元素, 如果存在域  $F(A)$  上  $m$  个不定元  $Y_1, \dots, Y_m$  的多项式

$$f(Y_1, \dots, Y_m) = \sum_{(i)} c_{(i)} Y_1^{i_1} \cdots Y_m^{i_m},$$

$c_{(i)} = c_{i_1, \dots, i_m} \in F(A)$ , 使得  $f(\eta_1, \dots, \eta_m) = 0$ , 我们证明, 所有系数  $c_{(i)} = 0$ .  $c_{(i)} \in F(A)$  是  $F$  上关于  $A$  的元素的有理分式, 因为只有有限个  $c_{(i)}$ , 所以存在  $\xi_1, \dots, \xi_n \in A$  和  $u_{(i)} = u_{(i)}(X_1, \dots, X_n)$ ,  $v = v(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$ , 且  $v(\xi_1, \dots, \xi_n) \neq 0$  使得每一个  $c_{(i)}$  都可以表成

$$c_{(i)} = u_{(i)}(\xi_1, \dots, \xi_n) / v(\xi_1, \dots, \xi_n).$$

因为  $f(\eta_1, \dots, \eta_m) = \sum_{(i)} c_{(i)} \eta_1^{i_1} \cdots \eta_m^{i_m} = 0$ , 所以

$$\sum_{(i)} v_{(i)}(\xi_1, \dots, \xi_n) \eta_1^{i_1} \cdots \eta_m^{i_m} = 0.$$

令

$$\begin{aligned} g &= g(X_1, \dots, X_n, Y_1, \dots, Y_m) = \\ &= \sum_{(i)} u_{(i)}(X_1, \dots, X_n) Y_1^{i_1} \dots Y_m^{i_m}. \end{aligned}$$

$g$  是  $F$  上  $n+m$  个不定元  $X_1, \dots, X_n, Y_1, \dots, Y_m$  的多项式. 我们有

$$g(\xi_1, \dots, \xi_n, \eta_1, \dots, \eta_m) = 0.$$

因为  $A \cup B$  在  $F$  上代数无关, 且  $A \cap B = \emptyset$ ,  $\xi_1, \dots, \xi_n, \eta_1, \dots, \eta_m$  是  $A \cup B$  中互不相同的元素, 因而在  $F$  上代数无关. 所以  $g$  中系数必须全为零, 由此得

$$u_{(i)}(X_1, \dots, X_n) = 0.$$

于是

$$c_{(i)} = u_{(i)}(\xi_1, \dots, \xi_n) / v(\xi_1, \dots, \xi_n) = 0,$$

从而  $f(Y_1, \dots, Y_m) = 0$ . 这就证明了  $B$  在  $F(A)$  上代数无关.

(ii)  $\implies$  (i) 设  $A$  在  $F$  上代数无关,  $B$  在  $F(A)$  上代数无关. 如果有  $c \in A \cap B$ , 那么  $f(X) = X - c \in F(A)[X]$  而  $f(c) = 0$ . 因而  $c \in B$  是  $F(A)$  上代数元. 这与  $B$  在  $F(A)$  上代数无关的假设矛盾. 因此  $A \cap B = \emptyset$ .

现在证明  $A \cup B$  在  $F$  上代数无关. 设  $\xi_1, \dots, \xi_n, \eta_1, \dots, \eta_m$  是  $A \cup B$  中任意  $n+m$  个元素, 其中  $\xi_1, \dots, \xi_n \in A, \eta_1, \dots, \eta_m \in B$ , 我们证明, 如果有  $F$  上  $n+m$  个不定元  $X_1, \dots, X_n, Y_1, \dots, Y_m$  的多项式  $g(X_1, \dots, X_n, Y_1, \dots, Y_m)$ , 使得

$$g(\xi_1, \dots, \xi_n, \eta_1, \dots, \eta_m) = 0,$$

则  $g = 0$ .

当  $n = 0$  或  $m = 0$  时, 显然  $g = 0$ , 因此  $A$  和  $B$  都在  $F$  上代数无关.

设  $n \geq 1$  且  $m \geq 1$ , 将  $g$  写成多项式环  $F[X_1, \dots, X_n]$  上关于  $Y_1, \dots, Y_m$  的多项式:

$$g = \sum_{(i)} u_{(i)}(X_1, \dots, X_n) Y_1^{i_1} \dots Y_m^{i_m},$$

$u_{(i)}(X_1, \dots, X_n) = u_{i_1 \dots i_m}(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$ . 令

$$f(Y_1, \dots, Y_m) = \sum_{(i)} u_{(i)}(\xi_1, \dots, \xi_n) Y_1^{i_1} \dots Y_m^{i_m},$$

则  $f(Y_1, \dots, Y_m) \in F(A)[Y_1, \dots, Y_m]$ , 因为  $B$  在  $F(A)$  上代数无关, 所以

$$f(\eta_1, \dots, \eta_m) = 0 \implies u_{(i)}(\xi_1, \dots, \xi_n) = 0, \forall (i).$$

又因为  $\xi_1, \dots, \xi_n$  在  $F$  上代数无关, 所以  $u_{(i)}(X_1, \dots, X_n) = 0, \forall (i)$ . 于是

$$g(X_1, \dots, X_n, Y_1, \dots, Y_m) = 0.$$

所以  $A \cup B$  在  $F$  上代数无关. ■

设  $K$  是域  $F$  的一个扩域.  $K$  的一个子集  $B$  叫做  $K$  在  $F$  上一个**超越基**, 如果下列两条件被满足:

1.  $B$  在  $F$  上代数无关;
2.  $K$  是  $F(B)$  的代数扩域.

如果存在  $K$  在  $F$  上超越基  $B$ , 使得  $K = F(B)$ , 那么就说  $K$  是  $F$  的一个**纯超越扩域**, 而  $K/F$  称为一个**纯超越扩张**.

我们证明超越基的存在性 (可能是空集). 为此, 只需证明以下的

**定理 4.1.2** 设  $K$  是域  $F$  的一个扩域,  $A$  和  $C$  是  $K$  的子集, 且  $A \subseteq C$ .  $A$  在  $F$  上代数无关而  $K$  是  $F(C)$  的代数扩域. 那么存在  $K$  在  $F$  上的一个超越基  $B$ ,  $A \subseteq B \subseteq C$ .

**证** 令  $S = \{B' \subseteq K \mid A \subseteq B' \subseteq C, B' \text{ 在 } F \text{ 上代数无关}\}$ . 显然  $A \in S$ , 所以  $S \neq \emptyset$ . 对于集合的包含关系来说,  $S$  作成是一个偏序集. 设  $\{B_\lambda \mid \lambda \in \Lambda\}$  是  $S$  中一个链 ( $\Lambda$  是一个指标集). 令  $B^* = \bigcup_{\lambda \in \Lambda} B_\lambda$ . 则  $A \subseteq B^* \subseteq C$ . 设  $\xi_1, \dots, \xi_m$  是  $B^*$  中任意有限个元素.

那么存在某一个  $B_\lambda, \lambda \in \Lambda$ , 使得  $\xi_1, \dots, \xi_m \in B_\lambda$ . 因为  $B_\lambda$  在  $F$  上代数无关, 所以  $\xi_1, \dots, \xi_m$  在  $F$  上代数无关, 因而  $B^*$  在  $F$  上代数

无关, 所以  $B^* \in S$ . 显然对于任意  $\lambda \in A$ ,  $B^* \supseteq B_\lambda$ . 所以  $B^*$  是  $\{B_\lambda \mid \lambda \in A\}$  的一个上界. 因此  $S$  是归纳集. 于是由 Zorn 引理,  $S$  有一个极大元  $B$ .  $A \subseteq B \subseteq C$ .

我们证明,  $B$  就是  $K$  在  $F$  上一个超越基. 首先,  $B \in S$ , 所以  $B$  在  $F$  上代数无关. 其次, 我们有  $F(B) \subseteq F(C) \subseteq K$ , 而  $K$  是  $F(C)$  的代数扩域. 这样, 我们只需证明  $F(C)$  是  $F(B)$  的代数扩域即可. 如果有  $\xi \in F(C)$  而  $\xi$  是  $F(B)$  上超越元, 那么集  $\{\xi\}$  在  $F(B)$  上代数无关, 且  $\xi \notin B$  而  $B$  又在  $F$  上代数无关, 于是由 4.1.1,  $B \cup \{\xi\}$  在  $F$  上代数无关. 我们有

$$A \subseteq B \cup \{\xi\} \subseteq C,$$

所以  $B \cup \{\xi\} \in S$ . 然而  $\xi \notin B$ , 所以  $B \subsetneq B \cup \{\xi\}$ , 这与  $B$  是  $S$  的极大元的事实相矛盾. 于是,  $C$  在  $F(B)$  上是代数的, 从而  $F(C)$  是  $F(B)$  的代数扩域. 这就证明了  $K$  是  $F(B)$  的代数扩域.  $B$  是  $K$  在  $F$  上一个超越基. ■

**推论 4.1.3** 域  $F$  的任意一个扩域  $K$  都存在  $F$  上的超越基.

**证** 在 4.1.2 里, 取  $A = \emptyset$ ,  $C = K$ . ■

**推论 4.1.4** 设  $F$  是一个域,  $K$  是对  $F$  添加一个集  $C$  所得的扩域,  $K = F(C)$ , 那么一定存在  $K$  在  $F$  上一个超越基  $B$ , 且  $B \subseteq C$ .

**证** 在 4.1.2 里, 取  $A = \emptyset$ . ■

域  $F$  的一个扩域  $K$  在  $F$  上的超越基并不是唯一的. 自然发生这样的问题: 给了  $K$  在  $F$  上两个超越基  $B$  和  $C$ . 它们的基数是否相同? 下面将对这个问题作出肯定的回答.

以下我们用  $|B|$  表示一个集  $B$  的基数.

先考虑一个简单的情形, 即  $K$  在  $F$  上有一个超越基是有限集的情形. 这时我们有

**引理 4.1.5** 设  $K$  是域  $F$  的一个扩域. 如果  $K$  在  $F$  上有一个超越基  $B$  含有  $n$  个元素 ( $n$  是一个非负整数), 那么  $K$  在  $F$  上任意超越基都含有  $n$  个元素.

证 设  $B'$  是  $K$  在  $F$  上任意一个超越基. 我们证明  $|B'| \leq n \leq |B|$ . 由此, 对调  $B$  与  $B'$  的地位, 又有  $|B| \leq |B'|$ , 从而  $|B| = |B'|$ .

当  $n = 0$  时,  $B = \emptyset$ , 这时  $K$  是  $F$  的代数扩域. 所以  $K$  不含  $F$  上的超越元素, 因而  $|B'| = 0$ .

设  $n > 0$ , 假设对于任意域扩张  $L/M$  来说, 只要有一个超越基  $B_1$ , 而  $|B_1| = k < n$ , 那么对于  $L/M$  的任意超越基  $B'_1$ , 就有  $|B'_1| \leq k$ .

现在设  $B'$  是  $K$  在  $F$  上任意一个超越基. 如果  $B' \subseteq B$ , 那么自然有  $|B'| \leq n$ . 设  $B' \not\subseteq B$ , 那么存在  $\xi \in B'$  而  $\xi \notin B$ . 集  $\{\xi\}$  在  $F$  上代数无关, 又  $F(B) \subseteq F(B \cup \{\xi\}) \subseteq K$ , 而  $K$  是  $F(B)$  的代数扩域, 所以  $K$  是  $F(B \cup \{\xi\})$  的代数扩域. 由 4.1.2, 存在  $K$  在  $F$  上一个超越基  $\bar{B}$ , 使得  $\{\xi\} \subseteq \bar{B} \subseteq B \cup \{\xi\}$ . 记  $\bar{B} = C \cup \{\xi\}$ , 则  $C \subseteq B$ . 因为  $K$  是  $F(B)$  的代数扩域, 所以  $\xi$  是  $F(B)$  上代数元. 由 4.1.1,  $B \cup \{\xi\}$  在  $F$  上不是代数无关的. 然而  $\bar{B} = C \cup \{\xi\} \subseteq B \cup \{\xi\}$ , 所以  $C \subsetneq B$ . 因此  $|C| < |B| = n$ .

令  $F' = F(\xi)$ . 我们证明,  $C$  与  $B'' = B' \setminus \{\xi\}$  都是  $K$  在  $F'$  上的超越基.

事实上, 因为  $\bar{B} = C \cup \{\xi\}$  在  $F$  上代数无关, 由 4.1.1,  $C$  在  $F' = F(\xi)$  上代数无关. 其次,  $F'(C) = F(\bar{B})$ , 而  $K$  是  $F(\bar{B})$  上代数扩域, 所以  $K$  是  $F'(C)$  上代数扩域. 因此  $C$  是  $K$  在  $F'$  上一个超越基.

同理可证  $B'' = B' \setminus \{\xi\}$  也是  $K$  在  $F'$  上一个超越基.

由于  $|C| < n$ . 又由归纳法假设  $|B''| \leq |C|$ , 所以  $|B'| = |B''| + 1 \leq |C| + 1 \leq n$ . 引理被证明. ■

现在证明一般的

**定理 4.1.6** 设  $K$  是域  $F$  的一个扩域.  $K$  在  $F$  上任意两个超越基都有相同的基数.



证 设  $B$  和  $C$  是  $K/F$  的两个超越基. 如果  $B$  与  $C$  之一是有有限集, 那么由 4.1.5, 另一个也是有限集, 并且  $|B| = |C|$ .

现在设  $B$  与  $C$  都是无限集.

设  $\gamma \in C$ . 因为  $B$  是  $K/F$  的超越基, 所以  $\gamma$  是  $F(B)$  上代数元. 因此  $\gamma$  是系数在  $F(B)$  内的某个多项式

$$f(X) = \sum_{i=0}^m c_i X^i, \quad c_i \in F(B), c_m = 1,$$

的根. 存在  $\xi_1, \dots, \xi_l \in B$  和多项式  $u_i(X_1, \dots, X_l), 1 \leq i \leq m-1$ ,  $v(X_1, \dots, X_l) \in F[X_1, \dots, X_l]$ ,  $v(\xi_1, \dots, \xi_l) \neq 0$  使得,

$$c_i = u_i(\xi_1, \dots, \xi_l) / v(\xi_1, \dots, \xi_l), \quad 1 \leq i \leq m-1.$$

因此,  $f(X)$  是系数在  $F(\xi_1, \dots, \xi_l)$  内的多项式. 令  $B_\gamma = \{\xi_1, \dots, \xi_l\} \subseteq B$ , 则  $\gamma$  是  $F(B_\gamma)$  上代数元.

这样, 对于  $C$  的每一个元素  $\gamma$ , 可以选取  $B$  的一个有限子集  $B_\gamma$ , 使得  $\gamma$  是  $F(B_\gamma)$  上的代数元.

显然  $\bigcup_{\gamma \in C} B_\gamma \subseteq B$ . 假设存在  $\beta \in B$  而  $\beta \notin \bigcup_{\gamma \in C} B_\gamma$ . 由于  $C$  是  $K/F$  的超越基, 所以  $\beta$  是  $F(C)$  上代数元. 另一方面,  $C$  的每一个元素都是  $F(\bigcup_{\gamma \in C} B_\gamma)$  上的代数元, 所以  $F(C)$  是  $F(\bigcup_{\gamma \in C} B_\gamma)$  的代数扩域. 因此  $\beta$  是  $F(\bigcup_{\gamma \in C} B_\gamma)$  上的代数元. 然而  $\beta \notin \bigcup_{\gamma \in C} B_\gamma$ , 所以由 4.1.1,  $B$  的子集  $(\bigcup_{\gamma \in C} B_\gamma) \cup \{\beta\}$  在  $F$  上不是代数无关的, 这与  $B$  是  $K/F$  的超越基的假设矛盾. 这样就有  $B = \bigcup_{\gamma \in C} B_\gamma$ .

因为  $C$  是无限集, 而每一个  $B_\gamma$  都是有限集, 所以我们有

$$|B| = \left| \bigcup_{\gamma \in C} B_\gamma \right| \leq \aleph_0 \cdot |C| = |C|,$$

这里  $\aleph_0$  表示可数集的基数.

对调  $B$  与  $C$  的地位, 我们又有  $|C| \leq |B|$ . 因此  $|B| = |C|$ . ■

定理 4.1.6 表明, 域扩张  $K/F$  的任意两个超越基都具有相同的基数. 我们把这唯一确定的基数定义为  $K$  在  $F$  上的超越次数, 记作  $\text{tr.deg}_F K$  或  $\text{tr.deg}(K/F)$ .

定理 4.1.7 设  $K$  是域  $F$  的一个扩域.

(i)  $K/F$  是代数扩张  $\iff \text{tr.deg}_F K = 0$ .

(ii) 设  $K$  是对  $F$  添加  $n$  ( $n \geq 0$ ) 个元素  $\alpha_1, \dots, \alpha_n$  所生成的:  $K = F(\alpha_1, \dots, \alpha_n)$ . 那么  $\text{tr.deg}_F K \leq n$ .

证 (i)  $K/F$  是代数扩张  $\iff K/F$  的超越基是空集  $\iff \text{tr.deg}_F K = 0$ .

(ii) 由 4.1.4, 存在  $K/F$  的超越基  $B$ , 使得  $B \subseteq \{\alpha_1, \dots, \alpha_n\}$ . 所以  $\text{tr.deg}_F K \leq n$ . ■

定理 4.1.8 设  $K$  是域  $F$  的一个扩域, 且  $\text{tr.deg}_F K = n$ .

(i)  $K$  的子集  $A$  如果在  $F$  上代数无关, 则  $|A| \leq n$ .  $|A| = n \iff A$  是  $K/F$  的一个超越基.

(ii) 设  $C$  是  $K$  的一个子集而  $K$  是  $F(C)$  的代数扩域, 则  $|C| \geq n$ .  $|C| = n \iff C$  是  $K/F$  的一个超越基.

证 (i) 由 4.1.2, 存在  $K/F$  的超越基  $B$ , 使得  $A \subseteq B$ . 因此  $|A| \leq |B| = n$ .  $|A| = n \iff A = B$ .

(ii) 如同 (i) 一样, 由 4.1.2 存在  $K/F$  的超越基  $B$  使得  $B \subseteq C$ . 所以  $n = |B| \leq |C|$ .  $|C| = n \iff C = B$ . ■

定理 4.1.9 设  $F \subseteq K \subseteq L$  是一串扩域. 我们有

$$\text{tr.deg}_F L = \text{tr.deg}_K L + \text{tr.deg}_F K.$$

证 设  $B$  是  $K/F$  的一个超越基,  $C$  是  $L/K$  的一个超越基. 我们证明,  $B \cup C$  是  $L/F$  的一个超越基, 且  $B \cap C = \emptyset$ .

因为  $B$  在  $F$  上代数无关,  $C$  在  $K$  上代数无关, 所以  $C$  在  $F(B)$  上代数无关. 由 4.1.1,  $B \cap C = \emptyset$ , 且  $B \cup C$  在  $F$  上代数无关. 为了证明  $B \cup C$  是  $L/F$  的一个超越基, 只需证明  $L$  是  $F(B \cup C)$  上的代数扩域.

因为  $K$  是  $F(B)$  上的代数扩域, 所以  $K$  的元素是  $F(B \cup C)$  上的代数元, 因而域  $K(B \cup C) = F(B \cup C)(K)$  是  $F(B \cup C)$  上的代数扩域. 另一方面,  $K(C) \subseteq K(B \cup C) \subseteq L$ , 而  $L$  是  $K(C)$  上的代数扩域, 所以也是  $K(B \cup C)$  上的代数扩域. 于是  $L$  是  $F(B \cup C)$  上的代数扩域. 这就证明了  $B \cup C$  是  $L/F$  的一个超越基. 于是

$$\begin{aligned} \text{tr.deg}_F L &= |B \cup C| = |B| + |C| = \\ &= \text{tr.deg}_F K + \text{tr.deg}_K L. \end{aligned}$$

**推论 4.1.10** 设  $L$  是域  $F$  的一个扩域, 而  $K$  是  $L/F$  的一个中间域. 那么  $\text{tr.deg}_F K \leq \text{tr.deg}_F L$ . ■

**定理 4.1.11** 设  $M$  是域  $F$  的一个扩域,  $K$  和  $L$  都是  $M/F$  的中间域,  $KL$  是  $K$  与  $L$  的合成域. 那么

$$\begin{aligned} \text{tr.deg}_K KL &\leq \text{tr.deg}_F L; \quad \text{tr.deg}_L KL \leq \text{tr.deg}_F K; \\ \text{tr.deg}_F KL &\leq \text{tr.deg}_F K + \text{tr.deg}_F L. \end{aligned}$$

**证** 令  $B$  是  $L/F$  的一个超越基.  $L$  的每一个元素都是  $F(B)$  上的代数元, 所以  $KL = K(L)$  是  $K(B)$  上的代数扩域. 由 4.1.2, 存在  $KL/K$  的一个超越基  $C$ , 且  $C \subseteq B$ . 于是

$$\text{tr.deg}_K KL = |C| \leq |B| = \text{tr.deg}_F L.$$

同理有

$$\text{tr.deg}_L KL \leq \text{tr.deg}_F K.$$

再由 4.1.9,

$$\begin{aligned} \text{tr.deg}_F KL &= \text{tr.deg}_F K + \text{tr.deg}_K KL \\ &\leq \text{tr.deg}_F K + \text{tr.deg}_F L. \end{aligned}$$

在 2.3 里, 我们定义域  $F$  的正规扩域  $E$  是满足是以下两个条件的一个扩域:

1.  $E$  是  $F$  的代数扩域;
2.  $E$  在  $F$  上的每一个共轭域都等于  $E$ .

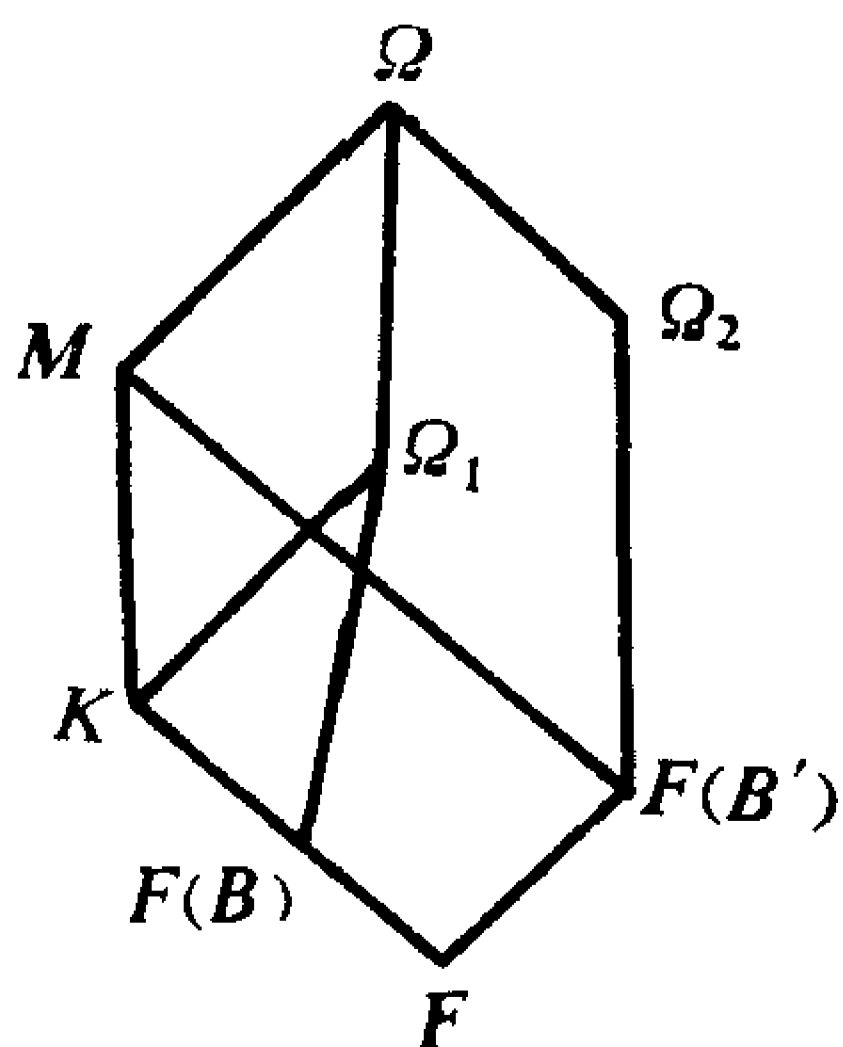
下面的定理表明, 在正规扩域的定义里, 条件 1 是多余的.

**定理 4.1.12** 设  $K$  是域  $F$  的一个扩域. 如果  $K$  在  $F$  上每一

个共轭域都等于 $K$ 本身, 则 $K$ 是 $F$ 的代数扩域.

证 假设 $K$ 是 $F$ 的超越扩域. 我们证明, 存在 $K$ 的一个扩域 $\Omega$ 和一个 $K$ 到 $\Omega$ 内的 $F$ -共轭 $\sigma: K \rightarrow \Omega$ , 使得 $\sigma(K) \neq K$ .

令 $B = \{\xi_\lambda\}_{\lambda \in \Lambda}$ 是 $K/F$ 的一个超越基. 令 $B' = \{X_\lambda\}_{\lambda \in \Lambda}$ 是与 $B$ 具有同一指标集 $\Lambda$ 的 $K$ 上不相关不定元的集. 令 $M = K(B')$ 是 $K$ 上关于 $B' = \{X_\lambda\}_{\lambda \in \Lambda}$ 的有理分式域 (即 $K$ 上关于 $B'$ 的一切有限子集的有理分式域的并集). 我们有 $F \subseteq F(B) \subseteq K \subseteq M$ .



令 $\Omega$ 是 $M$ 的一个代数闭包, 令 $\Omega_1$ 是 $F(B)$ 在 $\Omega$ 内的代数闭包,  $\Omega_2$ 是 $F(B')$ 在 $\Omega$ 内的代数闭包.

集 $B = \{\xi_\lambda\}_{\lambda \in \Lambda}$ 在 $F$ 上代数无关, 所以存在 $F$ -同构

$$\varphi: F(B) \xrightarrow{\sim} F(B'),$$

$$\varphi(\xi_\lambda) = X_\lambda, \lambda \in \Lambda.$$

$\varphi$ 可以开拓为 $F(B)$ 的代数闭包 $\Omega_1$ 到 $F(B')$ 的代数闭包 $\Omega_2$ 的一个 $F$ -同构, 仍用 $\varphi$ 来表示这个开拓. 令

$K' = \varphi(K) \subseteq \Omega_2$ . 由 $\{X_\lambda\}_{\lambda \in \Lambda}$ 的取法和 $\varphi$ 的作法, 我们有 $\sigma = \varphi|_K: K \rightarrow \Omega$ 是 $K$ 到 $\Omega$ 的一个 $F$ -共轭.  $X_\lambda = \varphi(\xi_\lambda) \in K'$ 但 $X_\lambda \notin K$ , 所以 $K' \neq K$ . 这与题设相矛盾. ■

## 习 题

1. 令 $K$ 是域 $F$ 的一个扩域,  $S$ 是 $K$ 的一个子集. 设 $\alpha \in K$ 在 $F(S)$ 上是代数的, 而 $\alpha$ 在 $F(S \setminus \{\beta\})$ 上不是代数的, 其中 $\beta \in S$ . 证明,  $\beta$ 在 $F((S \setminus \{\alpha\}) \cup \{\beta\})$ 上是代数的.

2. 设 $K$ 是域 $F$ 的一个扩域,  $A$ 和 $C$ 都是 $K$ 的子集, 其中 $A$ 在 $F$ 上代数无关而 $K$ 是 $F(C)$ 的代数扩域. 那么存在 $C$ 的一个子集 $C'$ , 使得 $A \cap C' = \emptyset$ 且 $B = A \cup C'$ 是 $K$ 在 $F$ 上一个超越基.

3. (i) 设  $B$  是复数域  $C$  在有理数域  $Q$  上一个超越基. 则  $B$  是无限集.

(ii) 证明,  $C$  有无限多个互不相同的自同构.

(iii) 证明,  $\text{tr.deg}_Q C = |C|$ .

4. 设  $F$  是一个代数闭域  $\Omega$  的子域,  $K$  是  $\Omega/F$  的一个中间域, 且  $\text{tr.deg}_F K$  是有限的. 证明,  $K$  到  $\Omega$  内的任意一个  $F$ -同态单射都可以开拓成为  $\Omega$  的一个自同构.

5. 如果在习题 4 里, 去掉  $\text{tr.deg}_F K$  是有限的条件, 习题 4 的结论是否还成立?

6. 设  $K = F(X_1, \dots, X_n)$  是域  $F$  上  $n$  个不定元的有理分式域,  $S_n$  和  $A_n$  分别是  $n$  次对称群和  $n$  次交错群. 对于  $\sigma \in S_n$ ,  $f(X_1, \dots, X_n) \in K$ , 定义

$$\sigma(f(X_1, \dots, X_n)) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

则  $\sigma$  是  $K$  的一个自同构. 令

$$L = \{f \in K \mid \sigma(f) = f, \forall \sigma \in S_n\};$$

$$M = \{f \in K \mid \sigma(f) = f, \forall \sigma \in A_n\}.$$

证明,  $L$  和  $M$  都是  $F$  上超越次数为  $n$  的纯超越扩域.

## 4.2 Lüroth 定理

一个域  $F$  上的纯超越扩域, 特别是有限生成的纯超越扩域, 看起来是比较简单的. 我们知道,  $F$  上任意一个有限生成的纯超越扩域  $K$  都与  $F$  上  $n$  个不定元  $X_1, \dots, X_n$  的有理分式域  $F(X_1, \dots, X_n)$  同构. 然而尽管如此, 一般说来, 一个纯超越扩张  $K/F$  的中间域是什么样子还不容易弄清楚. 在这一节里, 我们将对于最简单的纯超越扩张, 也就是超越次数是 1 的纯超越扩张, 给出它的中间域的结构.

先证两个引理.

**引理 4.2.1** 设  $X$  和  $Y$  是域  $F$  上不相关不定元,  $f(X), g(X)$

是一对互素的多项式. 那么多项式  $g(X)Y - f(X)$  是  $F(Y)[X]$  的不可约多项式.

证  $R = F[X]$  是唯一因式分解整环, 多项式  $g(X)Y - f(X)$  是  $R[Y]$  中的本原多项式, 并且是  $R$  的商域  $F(X)$  上关于  $Y$  的一次多项式, 因而是  $R[Y]$  的不可约的本原多项式. 所以  $g(X)Y - f(X)$  是  $R[Y] = F[X, Y]$  中关于两个文字  $X, Y$  的不可约多项式, 又因为  $F[Y]$  是唯一因式分解整环, 所以  $g(X)Y - f(X)$  是  $F[Y]$  的商域  $F(Y)$  上关于  $X$  的不可约多项式. ■

**引理 4.2.2** 设  $F$  是一个域,  $K = F(x)$ ,  $x$  是  $F$  上一个超越元;  $u \in K$  但  $u \notin F$ ,  $u = f(x)/g(x)$ , 其中  $f(x), g(x) \in F[x]$  是互素的多项式. 那么  $K$  是  $F(u)$  上有限次扩域, 并且

$$[K : F(u)] = \max(\deg f(x), \deg g(x)).$$

证  $u$  是  $F$  上超越元 (见 2.1.9). 考虑  $F(u)$  上关于不定元  $T$  的多项式

$$\varphi(T) = g(T)u - f(T).$$

则  $f(T), g(T) \in F[T]$ , 且  $(f(T), g(T)) = 1$ . 由 4.2.1,  $\varphi(T)$  是  $F(u)$  上不可约多项式. 我们有

$$\varphi(x) = g(x)u - f(x) = 0.$$

所以  $x$  是  $F(u)$  上代数元, 并且

$$[K : F(u)] = [F(x) : F(u)] = \deg \varphi(T).$$

因为  $u$  是  $F$  上的超越元, 所以在  $\varphi(T) = g(T)u - f(T)$  中,  $g(T)u$  与  $f(T)$  中关于  $T$  的同次项的系数不能互相抵消. 于是

$$\deg \varphi(T) = \max(\deg f(T), \deg g(T)).$$
 ■

现在我们证明以下

**定理 4.2.3 (Lüroth)** 设  $K = F(x)$  是域  $F$  的一个纯超越扩域,  $E$  是  $K/F$  的一个中间域, 且  $E \neq F$ . 那么存在  $F$  上一个超越元  $t$ , 使得  $E = F(t)$ .

证 因为  $F \subsetneq E$ , 所以存在  $u \in E$ , 但  $u \notin F$ . 由 4.2.2,  $K$  是

$F(u)$ 的有限次扩域, 因而是 $E$ 的有限次扩域, 所以 $K$ 是 $E$ 的代数扩域, 令 $x \in K$ 在 $E$ 上的最小多项式是

$$f_0(T) = T^n + a_1 T^{n-1} + \cdots + a_n.$$

$a_i \in E \subseteq K$ . 每一个 $a_i$ 都是 $F$ 上关于 $x$ 的有理分式, 因此总可以表示成

$$a_i = a_i(x) = \frac{b_i(x)}{b_0(x)},$$

这里 $b_i(x), b_0(x) \in F[x], 1 \leq i \leq n$ , 且 $b_0(x), b_1(x), \dots, b_n(x)$ 是 $F[x]$ 中一组互素的多项式. 于是

$$f(x, T) = b_0(x)T^n + b_1(x)T^{n-1} + \cdots + b_n(x) \in F[x, T].$$

$f(x, T)$ 关于 $T$ 的次数是 $n$ . 又设 $f(x, T)$ 关于 $x$ 的次数是 $m$ .

因为 $x$ 是 $F$ 上的超越元, 所以 $a_1, \dots, a_n$ 中至少有某一个 $a_i$ 不属于 $F$ . 我们将这个 $a_i$ 记作 $t$ .  $t = a_i \notin F$ . 则 $t$ 是 $F$ 上超越元 (2.1.9). 现在证明,  $E = F(t)$ .

将 $t = b_i(x)/b_0(x)$ 表示成 $F[x]$ 中两个互素多项式的商:

$$t = g(x)/h(x), g(x), h(x) \in F[x], (g(x), h(x)) = 1,$$

且 $g(x) \mid b_i(x), h(x) \mid b_0(x)$ , 于是 $\deg g(x) \leq m, \deg h(x) \leq m$ .

考虑 $E[T]$ 的多项式

$$g(T) - th(T) = g(T) - \frac{g(x)}{h(x)}h(T).$$

那么 $x$ 是这个多项式的一个根. 因此, 在 $E[T]$ 内,  $f_0(T)$ 整除 $g(T) - th(T)$ . 所以

$$g(T) - th(T) = f_0(T)q_0(T), q_0(T) \in E[T].$$

两边乘上 $F[x]$ 的一个适当的多项式, 我们可以得到

$$\varphi(x)(g(T)h(x) - g(x)h(T)) = f(x, T)q_0(x, T).$$

$\varphi(x) \in F[x], q_0(x, T) \in F[x, T]$ . 因为 $f(x, T)$ 没有 $F[x]$ 中次数大于零的因式, 所以在 $F[x, T]$ 里,  $\varphi(x)$ 整除 $q_0(x, T)$ . 因此, 存在 $q(x, T) \in F[x, T]$ , 使得

$$g(T)h(x) - g(x)h(T) = f(x, T)q(x, T).$$

等式左端关于  $x$  的次数至多为  $m$ ，而右端  $f(x, T)$  关于  $x$  的次数等于  $m$ ，因此只可能左端关于  $x$  的次数等于  $m$  并且右端  $q(x, T)$  关于  $x$  的次数等于 0。所以  $q(x, T) = q(T) \in F[T]$ 。

我们证明， $q(T) = c \in F$ 。假设  $\deg q(T) > 0$ 。令  $\alpha$  是  $q(T)$  的一个根（在  $F(x)$  的一个代数闭包内）。于是就有

$$g(\alpha)h(x) - g(x)h(\alpha) = f(x, 0)q(\alpha) = 0.$$

如果  $g(\alpha) = h(\alpha) = 0$ ，那么  $g(x)$  与  $h(x)$  可以同时被  $\alpha$  在  $F$  上的最小多项式整除，这与  $g(x), h(x)$  互素的假设矛盾。如果  $h(\alpha) \neq 0$ ，那么由上面的等式得出  $t = g(x)/h(x) = g(\alpha)/h(\alpha)$  是  $F$  上代数元，这又导致矛盾，如果  $g(\alpha) \neq 0$ ，我们又得到  $t^{-1} = h(\alpha)/g(\alpha)$ ，也同样导致矛盾。这样一来，只能是  $q(T) = c \in F$ 。于是

$$g(T)h(x) - g(x)h(T) = cf(x, T), \quad c \in F.$$

由左端的多项式的形状可以看出，它关于  $x$  的次数与关于  $T$  的次数是相同的，都等于  $m$ ，而右端关于  $T$  的次数是  $n$ 。因此  $m = n$ 。

另一方面，因为  $t \in E$ ，所以  $F(t) \subseteq E \subseteq K$ 。于是

$$[K : F(t)] \geq [K : E] = n = m.$$

再由 4.2.2， $[K : F(t)] = \max(\deg g(x), \deg h(x)) \leq m$ 。这样一来，就必须  $[K : F(t)] = [K : E]$ ，从而  $E = F(t)$ 。定理被证明。 ■

## 习 题

1. 设  $F$  是一个域， $K = F(x)$ ， $x$  是  $F$  上一个超越元。证明：

(i) 对于  $y \in K$  来说， $F(y) = F(x)$  必要且只要

$$y = \frac{ax + b}{cx + d},$$

$a, b, c, d \in F$  且  $ad - bc \neq 0$ 。



(ii)  $K$  的  $F$ -自同构群与  $F$  上二阶射影线性群  $PSL_2(F)$  同构, 这里  $PSL_2(F)$  定义为  $F$  上全体二阶可逆方阵对方阵的乘法所成的群对其中心的商群.

2. 设  $F$  是一个域,  $K = F(x, y)$ , 其中  $x$  是  $F$  上的超越元且  $x^2 + y^2 = 1$ , 证明  $K$  是  $F$  上的纯超越扩域.

3. 设  $F$  是一个域,  $\text{char } F \neq 2$ .  $K = F(x, y)$ , 其中  $x, y$  满足关系  $ax^2 + by^2 = 1$ ,  $a, b \in F$  且  $ab \neq 0$ . 证明以下两个条件等价:

(i) 存在  $t \in K$ , 使得  $K = F(t)$ ;

(ii) 方程  $aX^2 + bY^2 = Z^2$  在  $F$  中有一个非零解.

4. 设  $F$  是一个无限域,  $x_1, \dots, x_n$  是  $F$  上一组代数无关的元素, 而  $K$  是  $F(x_1, \dots, x_n)/F$  的一个中间域. 又设  $\text{tr. deg}_F K = r$ . 证明, 存在  $y_1, \dots, y_r$ , 使得  $K \subseteq F(y_1, \dots, y_r)$ .

[提示: 先设  $r=1$ , 对  $n$  作归纳法, 然后再对  $r$  作归纳法.]

5. 设  $F$  是一个特征不为 3 的域,  $x$  是  $F$  上一个超越元,  $K = F(x, y)$ , 且  $x^3 + y^3 = 1$ . 证明,  $K$  不是  $F$  上纯超越扩张.

### 4.3 线性无缘

为了以下的讨论, 在这一节里我们介绍域线性无缘的概念. 先证明以下的

**引理 4.3.1** 设  $M$  是域  $F$  的一个扩域.  $K$  和  $L$  都是  $M/F$  的中间域. 以下两个条件是等价的:

(i)  $K$  中任意一个在  $F$  上线性无关的子集也在  $L$  上线性无关;

(ii)  $L$  中任意一个在  $F$  上线性无关的子集也在  $K$  上线性无关.

**证** (i)  $\implies$  (ii) 令  $S$  是  $L$  的一个在  $F$  上线性无关的子集.  $\beta_1, \dots, \beta_m$  是  $S$  中任意有限个元素. 则  $\beta_1, \dots, \beta_m$  在  $F$  上线性无关. 如果有  $\alpha_1, \dots, \alpha_m \in K$ , 使得

$$\alpha_1 \beta_1 + \cdots + \alpha_m \beta_m = 0,$$

适当编号, 可设  $\alpha_1, \cdots, \alpha_n (n \leq m)$  在  $F$  上线性无关, 而每一个  $\alpha_i (1 \leq i \leq m)$  可以表示成  $\alpha_1, \cdots, \alpha_n$  的  $F$ -线性组合:

$$\alpha_i = \sum_{j=1}^n a_{ij} \alpha_j, \quad a_{ij} \in F,$$

于是

$$0 = \sum_{i=1}^m \alpha_i \beta_i = \sum_{j=1}^n \left( \sum_{i=1}^m a_{ij} \beta_i \right) \alpha_j = \sum_{j=1}^n \gamma_j \alpha_j,$$

$\gamma_j = \sum_{i=1}^m a_{ij} \beta_i \in L (1 \leq j \leq n)$ . 由 (i), 我们有  $\gamma_j = 0 (1 \leq j \leq n)$ .

从而  $a_{ij} = 0 (1 \leq i \leq m, 1 \leq j \leq n)$ . 所以  $\alpha_i = 0 (1 \leq i \leq m)$ . 这样,  $\beta_1, \cdots, \beta_m$  在  $L$  上线性无关, 即  $S$  在  $L$  上线性无关.

(ii)  $\implies$  (i) 证明完全类似. ■

设  $F$  是一个域,  $M$  是  $F$  的一个扩域,  $K$  和  $L$  是  $M/F$  的中间域. 如果引理中等价的两个条件之一被满足, 那么就说  $K$  与  $L$  在  $F$  上线性无缘.

由定义直接得到以下

**定理 4.3.2** 设  $M$  是域  $F$  的一个扩域,  $K$  和  $L$  是  $M/F$  的中间域. 以下条件是等价的:

(i)  $K$  与  $L$  在  $F$  上线性无缘;

(ii)  $K/F$  的任意中间域  $K'$  与  $L/F$  的任意中间域  $L'$  在  $F$  上线性无缘;

(iii)  $K$  的任意在  $F$  上有限生成的子域  $K'$  与  $L$  的任意在  $F$  上有限生成的子域  $L'$  在  $F$  上线性无缘;

(iv) 对于  $K$  中任意在  $F$  上线性无关的元素  $\alpha_1, \cdots, \alpha_m$  和  $L$  中任意在  $F$  上线性无关的元素  $\beta_1, \cdots, \beta_n$ , 乘积  $\alpha_i \beta_j, 1 \leq i \leq m, 1 \leq j \leq n$ , 也在  $F$  上线性无关.

**证** (i)  $\implies$  (ii), (ii)  $\implies$  (iii) 都是明显的.

(iii)  $\implies$  (iv) 令  $K' = F(\alpha_1, \cdots, \alpha_m), L' = F(\beta_1, \cdots, \beta_n)$ ,

则  $K'$  与  $L'$  在  $F$  上线性无缘。如果有  $F$  上线性关系

$$\sum_{i=1}^m \sum_{j=1}^n a_{ij} \alpha_i \beta_j = 0, a_{ij} \in F,$$

成立，那么由于  $\beta_1, \dots, \beta_m$  在  $K$  上线性无关，而  $\sum_{i=1}^m a_{ij} \alpha_i \in K$ ，所以  $\sum_{i=1}^m a_{ij} \alpha_i = 0$  ( $1 \leq j \leq n$ )。又因为  $\alpha_1, \dots, \alpha_m$  在  $F$  上线性无关，所以  $a_{ij} = 0$  ( $1 \leq i \leq m, 1 \leq j \leq n$ )。

(iv)  $\Rightarrow$  (i) 设  $S \subseteq K$  是任意一个在  $F$  上线性无关的子集。令  $\alpha_1, \dots, \alpha_m$  是  $S$  中任意有限个元素。如果有  $\beta_1, \dots, \beta_n \in L$ ，使得  $\sum_{i=1}^m \alpha_i \beta_i = 0$ ，适当编号，可以设  $\beta_1, \dots, \beta_n$  ( $n \leq m$ ) 在  $F$  上线性无关，而每一  $\beta_i$  ( $1 \leq i \leq m$ ) 可以由  $\beta_1, \dots, \beta_n$  线性表示：

$$\beta_i = \sum_{j=1}^n a_{ij} \beta_j \quad (1 \leq i \leq m).$$

于是 
$$\sum_{i=1}^m \sum_{j=1}^n a_{ij} \alpha_i \beta_j = 0.$$

由 (iv)，必须  $a_{ij} = 0$ ,  $1 \leq i \leq m, 1 \leq j \leq n$ 。因而  $K$  与  $L$  在  $F$  上线性无缘。 ■

**定理 4.3.3** 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域， $R$  是  $K$  的一个包含  $F$  的子整环，且  $K$  是  $R$  的商域。令  $\{\omega_i\}_{i \in I}$  是向量空间  $R$  在  $F$  上的一个基。那么  $K$  与  $L$  在  $F$  上线性无缘当且仅当  $\{\omega_i\}_{i \in I}$  在  $L$  上线性无关。

**证** 如果  $K$  与  $L$  在  $F$  上线性无缘，那么由 4.3.1,  $\{\omega_i\}_{i \in I}$  在  $L$  上线性无关。

反之，设  $\beta_1, \dots, \beta_m$  是  $L$  中任意有限个在  $F$  上线性无关的元素。假设存在  $\alpha_1, \dots, \alpha_m \in K$ ，使得  $\sum_{i=1}^m \alpha_i \beta_i = 0$ 。因为  $K$  是  $R$  的商域，我们可以用各  $\alpha_i$  ( $1 \leq i \leq m$ ) 的公分母去乘这个等式两端而得到等式

$$\sum_{i=1}^m \xi_i \beta_i = 0, \quad \xi_i \in R.$$

因为  $\{\omega_i\}_{i \in I}$  是  $R$  在  $F$  上的一个基, 所以存在有限个元素  $\omega_1, \dots, \omega_n \in \{\omega_i\}_{i \in I}$ , 使得

$$\xi_i = \sum_{j=1}^n a_{ij} \omega_j, \quad a_{ij} \in F.$$

于是

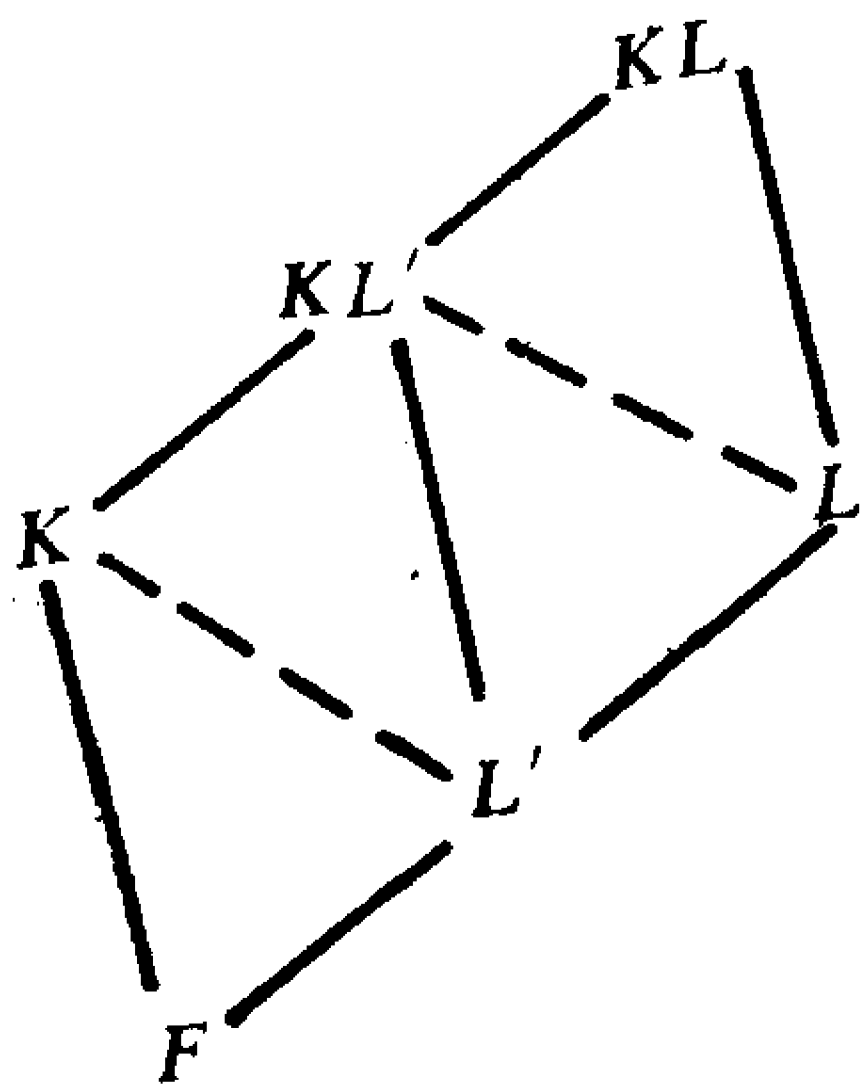
$$\sum_{i=1}^m \sum_{j=1}^n a_{ij} \omega_j \beta_i = 0.$$

因为  $\{\omega_i\}_{i \in I}$  在  $L$  上线性无关, 所以  $\sum_{i=1}^m a_{ij} \beta_i = 0, 1 \leq j \leq n$ . 而  $a_{ij} = 0 (1 \leq i \leq m, 1 \leq j \leq n)$ . 由此得出  $\alpha_i = 0 (1 \leq i \leq m)$ . 这就证明了  $K$  与  $L$  在  $F$  上线性无缘. ■

**推论 4.3.4** 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域,  $\{\omega_i\}_{i \in I}$  是  $K$  在  $F$  上一个基. 那么  $K$  与  $L$  在  $F$  上线性无缘当且仅当  $\{\omega_i\}_{i \in I}$  在  $L$  上线性无关. ■

**定理 4.3.5** 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域, 而  $L'$  是  $L/F$  的一个中间域. 那么  $K$  与  $L$  在  $F$  上线性无缘当且仅当以下两条件成立:

- (i)  $K$  与  $L'$  在  $F$  上线性无缘;
- (ii)  $KL'$  与  $L$  在  $L'$  上线性无缘.



**证** 假设条件 (i) 和 (ii) 成立. 设  $\{\omega_i\}_{i \in I}$  是  $K$  在  $F$  上一个基. 因为  $K$  与  $L'$  在  $F$  上线性无缘, 所以  $\{\omega_i\}_{i \in I}$  在  $L'$  上线性无关; 又因为  $KL'$  与  $L$  在  $L'$  上线性无缘, 所以  $\{\omega_i\}_{i \in I} (\subseteq KL')$  在  $L$  上线性无关.

于是由 4.3.4,  $K$  与  $L$  在  $F$  上线性无缘.

反过来, 设  $K$  与  $L$  在  $F$  上线性无缘. 这时条件 (i) 自然成立, 因为  $L' \subseteq L$ . 令  $\{\omega_i\}_{i \in I}$  是  $K$  在  $F$  上一个基, 那么  $\{\omega_i\}_{i \in I}$  在  $L$  上线性无关, 所以在  $L'$  上线性无关. 令

$$R = \left\{ \sum_{i \in I} \beta_i \omega_i \text{ (有限和)} \mid \beta_i \in L' \right\}$$

$R$  是  $L'$  上一个向量空间且  $\{\omega_i\}_{i \in I}$  是  $R$  在  $L'$  上一个基. 然而另一方面, 容易看出

$$R = \left\{ \sum_{i \in I} \alpha_i \beta_i \text{ (有限和)} \mid \alpha_i \in K, \beta_i \in L' \right\}.$$

是  $KL'$  的一个子整环, 并且  $KL'$  的元素都可以表示成  $\xi/\eta$  的形式,  $\xi, \eta \in R, \eta \neq 0$ . 因此  $KL'$  是  $R$  的商域, 于是由 4.3.3,  $KL'$  与  $L$  在  $L'$  上线性无缘. ■

## 习 题

1. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域, 并且  $[K:F] < \infty$ . 证明:

(i)  $KL/L$  是有限次扩张, 并且  $[KL:L] \leq [K:F]$ ;

(ii)  $[KL:L] = [K:F]$  必要且只要  $K$  与  $L$  在  $F$  上线性无缘.

2. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域. 证明:

(i)  $[KL:F] < \infty \iff [K:F] < \infty$  且  $[L:F] < \infty$ ;

(ii) 如果  $[KL:F] < \infty$ , 则  $[KL:F] \leq [K:F][L:F]$ ;

(iii) 如果  $[K:F]$  与  $[L:F]$  互素, 则  $[KL:F] = [K:F][L:F]$ , 并且这时  $K$  与  $L$  在  $F$  上线性无缘.

3. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域, 并且  $K/F$  是有限次 Galois 扩张. 证明,  $K$  与  $L$  在  $K \cap L$  上线性无缘. 如果  $K/F$  和  $L/F$  都不是 Galois 扩张, 上述断言是否仍成立?

4. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域, 其中  $K/F$  是纯超越扩张而  $L/F$  是代数扩张. 证明,  $K$  与  $L$  在  $F$  上线性无缘.

#### 4.4 域的代数无关性

设  $F$  是一个域,  $M$  是  $F$  的一个扩域. 在这一节里, 我们将讨论域扩张  $M/F$  的两个中间域在  $F$  上的代数无关性. 这是一个与线性无缘性既有区别又有联系的概念.

为了简单起见, 我们把  $M$  中的  $n$  个元素  $v_1, \dots, v_n$  所成的序组  $(v_1, \dots, v_n)$  简记作  $(v)$ . 设  $K$  是  $M$  的一个子域. 对  $K$  添加  $M$  的元素  $v_1, \dots, v_n$  所得的扩域  $K(v_1, \dots, v_n)$  简记作  $K(v)$ .

**引理 4.4.1** 设  $M$  是域  $F$  的一个扩域.  $K$  和  $L$  是  $M/F$  的中间域. 以下两个条件是等价的:

- (i)  $K$  的任意一个在  $F$  上代数无关的子集也在  $L$  上代数无关;
- (ii)  $L$  的任意一个在  $F$  上代数无关的子集也在  $K$  上代数无关.

**证** (i)  $\implies$  (ii) 设  $S$  是  $L$  的一个在  $F$  上代数无关的子集. 令  $v_1, \dots, v_n$  是  $S$  的任意有限个元素. 我们证明,  $v_1, \dots, v_n$  在  $K$  上代数无关.

记  $F(v) = F(v_1, \dots, v_n)$ . 因为  $v_1, \dots, v_n$  在  $F$  上代数无关, 所以  $\text{tr.deg}_F F(v) = n$ .

如果  $v_1, \dots, v_n$  在  $K$  上代数相关, 那么存在一个非零多项式  $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ , 使得  $f(v_1, \dots, v_n) = 0$ . 令  $\{\alpha_1, \dots, \alpha_m\}$  是  $f(X_1, \dots, X_n)$  的系数所成的集. 那么  $K' = F(\alpha_1, \dots, \alpha_m) \subseteq K$  是  $F$  上有限生成的扩域, 且  $f(X_1, \dots, X_n) \in K'[X_1, \dots, X_n]$ . 所以  $v_1, \dots, v_n$  在  $K'$  上代数相关. 于是

$$\text{tr.deg}_{K'} K'(v) < n.$$

设  $r = \text{tr.deg}_F K'$ , 而  $B' = \{y_1, \dots, y_r\}$  是  $K'$  在  $F$  上一个超越基. 因为  $B'$  在  $F$  上代数无关, 所以由 (i),  $B'$  也在  $F(v)$  ( $\subseteq L$ ) 上代数无关. 注意到  $K'(v) = K'F(v)$ , 于是

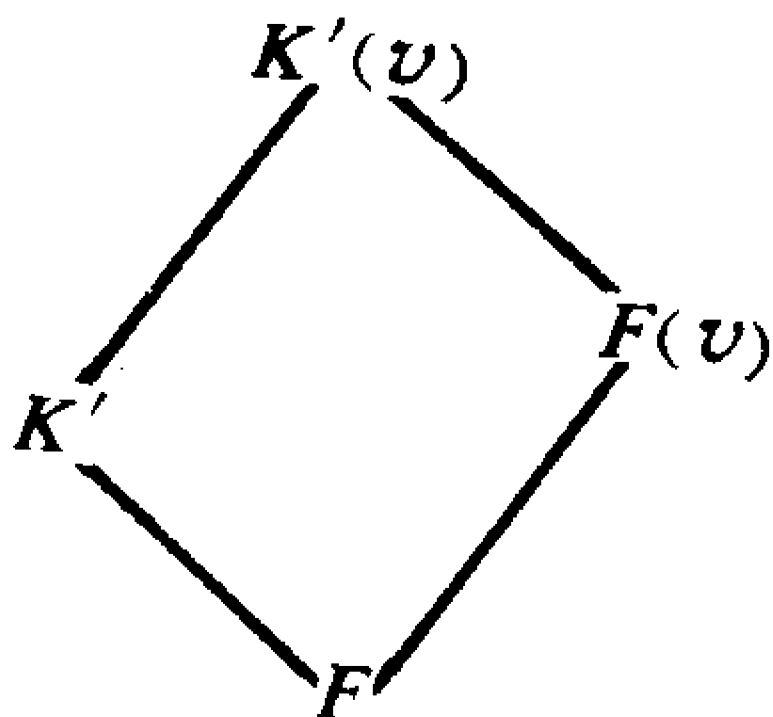
$$\text{tr.deg}_F K' = r \leq \text{tr.deg}_{F(v)} K'(v).$$

然而由 4.1.11, 我们有

$$\text{tr.deg}_{F(v)} K'(v) \leq \text{tr.deg}_F K' = r.$$

所以

$$\text{tr.deg}_{F(v)} K'(v) = r.$$



由以上结果, 按两种方法计算

$\text{tr.deg}_F K'(v)$ . 一方面,

$$\begin{aligned} \text{tr.deg}_F K'(v) &= \text{tr.deg}_{K'} K'(v) \\ &\quad + \text{tr.deg}_F K' < n + r; \end{aligned}$$

另一方面,

$$\begin{aligned} \text{tr.deg}_F K'(v) &= \text{tr.deg}_{F(v)} K'(v) \\ &\quad + \text{tr.deg}_F F(v) = r + n. \end{aligned}$$

这就导致矛盾. 因此  $v_1, \dots, v_n$  在  $K$  上代数无关.

(ii)  $\implies$  (i) 同样地证明. ■

设  $K$  和  $L$  是域扩张  $M/F$  的两个中间域. 如果 4.4.1 中两个等价的条件之一被满足, 那么就说  $K$  与  $L$  在  $F$  上代数无关.

**定理 4.4.2** 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域. 如果  $K$  与  $L$  在  $F$  上线性无缘, 则  $K$  与  $L$  在  $F$  上代数无关.

**证** 我们证明,  $K$  中任意有限个在  $F$  上代数无关的元素也在  $L$  上代数无关. 假设存在  $u_1, \dots, u_n \in K$ , 它们在  $F$  上代数无关而在  $L$  上代数相关, 那么存在  $L$  上多项式

$$f(X_1, \dots, X_n) = \sum_{(i)} c_{(i)} X_1^{i_1} \cdots X_n^{i_n} \neq 0,$$

$c_{(i)} = c_{i_1, \dots, i_n} \in L$ , 使得  $f(u_1, \dots, u_n) = 0$ . 因此, 出现在这个多项式中的所有单项式

$$\{M_{(i)}(u) = u_1^{i_1} \cdots u_n^{i_n}\} \subseteq K$$

在  $L$  上线性相关. 由假设,  $K$  与  $L$  在  $F$  上线性无缘, 所以这一组单项式  $\{M_{(i)}(u)\}$  在  $F$  上线性相关. 于是存在一个线性关系

$$\sum a_{(i)} M_{(i)}(u) = 0,$$

$a_{(i)} \in F$ , 并且不全为零. 令

$$h(X_1, \dots, X_n) = \sum a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \in F[X_1, \dots, X_n].$$

则  $h(X_1, \dots, X_n) \neq 0$ , 而  $h(u_1, \dots, u_n) = 0$ , 这与  $u_1, \dots, u_n$  在  $F$  上代数无关的假设矛盾. ■

**定理 4.4.3** 设  $K$  是域扩张  $M/F$  的中间域. 令  $(u) = (u_1, \dots, u_n)$  是  $M$  中一组在  $K$  上代数无关的元素. 那么  $K$  与  $F(u) = F(u_1, \dots, u_n)$  在  $F$  上线性无缘.

**证** 因为  $u_1, \dots, u_n$  在  $K$  上代数无关, 所以也在  $F$  上代数无关. 因此, 作为  $F$  上的向量空间, 一切单项式所成的集

$$\{u_1^{i_1} \cdots u_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{Z}_+\}$$

作成整环  $F[u] = F[u_1, \dots, u_n]$  在  $F$  上的一个基, 这里  $\mathbb{Z}_+$  表示全体非负整数集.

因为  $u_1, \dots, u_n$  在  $K$  上代数无关, 所以  $u_1, \dots, u_n$  的任意有限个单项式在  $K$  上线性无关, 所以  $F[u]$  的基  $\{u_1^{i_1} \cdots u_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{Z}_+\}$  在  $K$  上线性无关. 于是由 4.3.3,  $K$  与  $F(u)$  在  $F$  上线性无缘. ■

**定理 4.4.4** 设  $L$  是域  $F$  上一个有限生成的扩域. 那么  $L/F$  的任意中间域也是  $F$  上有限生成的.

**证** 设  $K$  是域扩张  $L/F$  的一个中间域. 我们区别两个情形来考虑.

**情形 1**  $K$  是  $F$  的代数扩域.

设  $L = F(u_1, \dots, u_n)$ . 适当编号, 可以假设  $u_1, \dots, u_s$  是  $L/F$  的一个超越基. 令  $E = F(u_1, \dots, u_s)$ . 则  $L = E(u_{s+1}, \dots, u_n)$  是  $E$  的代数扩域. 所以  $L$  是  $E$  的有限次扩域.

考虑合成域  $KE = K(u_1, \dots, u_s) = E(K)$ . 因为  $K$  是  $F$  的代数扩域, 所以  $K$  的每一个元素都是  $E$  上的代数元, 因此  $KE$  是  $E$  的代数扩域. 于是



$$\text{tr.deg}_F KE = \text{tr.deg}_E KE + \text{tr.deg}_F E = s.$$

另一方面,

$$\text{tr.deg}_F KE = \text{tr.deg}_K KE + \text{tr.deg}_F K = \text{tr.deg}_K KE.$$

所以  $\text{tr.deg}_K KE = s$ . 于是由 4.1.8,  $u_1, \dots, u_s$  在  $K$  上代数无关. 再由 4.4.3,  $K$  与  $E$  在  $F$  上线性无缘. 这样一来, 如果  $\alpha_1, \dots, \alpha_t$  是  $K$  在  $F$  上任意一组线性无关的元素, 那么  $\alpha_1, \dots, \alpha_t$  也在  $E$  上线性无关, 所以  $t \leq [L : E]$ . 因此

$$[K : F] \leq [L : E] < \infty.$$

所以  $K$  是  $F$  的有限次扩域, 因而是  $F$  上有限生成的扩域.

情形 2  $K$  不是  $F$  的代数扩域. 我们有

$$\text{tr.deg}_F K \leq \text{tr.deg}_F L < \infty.$$

令  $r = \text{tr.deg}_F K$ , 而  $u_1, \dots, u_r$  是  $K$  在  $F$  上一个超越基. 令  $F' = F(u_1, \dots, u_r)$ . 那么  $K$  是  $F'$  的代数扩域. 又  $L$  是  $F' (\supseteq F)$  上有限生成的, 于是由情形 1,  $K$  是  $F'$  上有限生成的. 因此, 存在  $v_1, \dots, v_s \in K$ , 使得  $K = F'(u_1, \dots, u_s)$ , 从而  $K = F(u_1, \dots, u_r, v_1, \dots, v_s)$  是  $F$  上有限生成的. ■

## 习 题

1. 设  $K$  是域扩张  $M/F$  的一个中间域.  $u_1, \dots, u_n \in M$ . 记  $(u) = (u_1, \dots, u_n)$ . 证明

$$\text{tr.deg}_K K(u) \leq \text{tr.deg}_F F(u).$$

当且仅当  $K$  与  $F(u)$  在  $F$  上代数无关时, 等号成立.

2. 设复数  $t$  是有理数域  $\mathbb{Q}$  上一个超越元.

$E = \mathbb{Q}(t)$ ,  $F = \mathbb{Q}(t+i) (i = \sqrt{-1})$ . 证明:

(i)  $E \cap F = \mathbb{Q}$ ;

(ii)  $E$  与  $F$  在  $\mathbb{Q}$  上不是代数无关的.

## 4.5 可分扩张

在第二章里，我们已经介绍了可分和不可分域扩张的概念。那时说到可分或不可分域扩张，都指的是代数扩张。现在我们将推广这个概念，讨论一般的可分扩张。

首先给出可分代数扩张的一个等价的定义。

**引理 4.5.1** 设  $F$  是一个特征为  $p > 0$  的域， $K$  是  $F$  的一个代数扩张。  $\Omega$  是  $K$  的一个代数闭包。令  $F^{1/p} = \{\alpha \in \Omega \mid \alpha^p \in F\}$ ， $F^{1/p}$  是  $\Omega/F$  的中间域。 $K$  是  $F$  的可分扩张必要且只要  $K$  与  $F^{1/p}$  在  $F$  上线性无缘。

**证** 设  $K$  是  $F$  的一个可分扩张。我们证明， $K$  的在  $F$  上任意的有限生成子域与  $F^{1/p}$  在  $F$  上线性无缘。

设  $F \subseteq E \subseteq K$ ， $E/F$  是有限生成的。则  $E$  是  $F$  上有限次可分扩张。于是由 2.1.3，存在  $\alpha \in E$ ，使得  $E = F(\alpha)$ 。令  $f(X) \in F[X]$  是  $\alpha$  在  $F$  上的最小多项式，则  $1, \alpha, \dots, \alpha^{n-1}$  ( $n = \deg f$ ) 作成  $E$  在  $F$  上一个基，于是根据 4.3.4，为了证明  $E$  与  $F^{1/p}$  在  $F$  上线性无缘，只需证明  $1, \alpha, \dots, \alpha^{n-1}$  在  $F^{1/p}$  上线性无关。

设  $h(X) \in F^{1/p}[X]$  是  $\alpha$  在  $F^{1/p}(\supseteq F)$  上的最小多项式。那么在  $F^{1/p}[X]$  内， $h(X) \mid f(X)$ ，另一方面  $h(X)^p \in F[X]$ ，所以在  $F[X]$  内， $f(X) \mid h(X)^p$ 。因为  $h(X)$  是  $F^{1/p}[X]$  里的不可约多项式，而  $f(X)$  是可分多项式，于是由  $F^{1/p}[X]$  内因式分解的唯一性得出  $f(X) = h(X)$ 。这样，

$$[F(\alpha) : F] = \deg f = \deg h = [F^{1/p}(\alpha) : F^{1/p}].$$

所以  $1, \alpha, \dots, \alpha^{n-1}$  在  $F^{1/p}$  上线性无关。

反过来，设  $K$  与  $F^{1/p}$  在  $F$  上线性无缘。我们证明， $K$  中任意元素  $\alpha$  都是  $F$  上的可分元素。

设  $\alpha \in K$ 。令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式， $\deg f = n$ 。则  $1, \alpha, \dots, \alpha^{n-1}$  在  $F$  上线性无关，而  $K$  与  $F^{1/p}$  在  $F$  上线性无缘，所

以  $1, \alpha, \dots, \alpha^{n-1}$  也在  $F^{1/p}$  上线性无关。如果  $\alpha$  不是  $F$  上的可分元素，那么存在  $g(X) \in F[X]$ ，使得  $f(X) = g(X^p)$ 。设

$$g(X) = \sum_{i=0}^m b_i X^i, \quad m = n/p.$$

则

$$h(X) = \sum_{i=0}^m b_i^{1/p} X^i \in F^{1/p}[X].$$

而

$$h(X)^p = g(X)^p = f(X).$$

于是  $h(\alpha)^p = f(\alpha) = 0$ ，从而  $h(\alpha) = 0$ 。这样一来， $1, \alpha, \dots, \alpha^m$  在  $F^{1/p}$  上线性相关。然而  $m = n/p < n$ 。这就导致矛盾。 ■

现在我们给出一般的可分扩张的定义。

设  $F$  是一个域， $\text{char} F = p$ ， $p$  是一个素数或 0。  $K$  是  $F$  的一个扩域， $\Omega$  是  $K$  的一个代数闭包。如果  $p = 0$ ，我们约定  $F^{1/p} = F$ ；如果  $p > 0$ ，令

$$F^{1/p} = \{\alpha \in \Omega \mid \alpha^p \in F\}.$$

域  $K$  叫做域  $F$  上一个可分扩域（域扩张  $K/F$  叫做可分扩张），如果  $K$  与  $F^{1/p}$  在  $F$  上线性无关。

根据这个定义，特征为 0 的域  $F$  的任意扩域都是  $F$  上的可分扩域。由 4.5.1，当  $K/F$  是代数扩张时，这个定义与在 2.7 所给的定义是一致的。

现在我们证明关于可分域扩张的几个等价的命题。

设  $F$  是一个域， $\text{char} F = p$ ， $p$  是一个素数或 0。  $K$  是  $F$  的一个扩域， $\Omega$  是  $K$  的一个代数闭包。  $\nu$  是一个非负整数。当  $p > 0$  时，定义

$$K^{p^\nu} = \{\alpha^{p^\nu} \mid \alpha \in K\},$$

$$F^{1/p^\nu} = \{\alpha \in \Omega \mid \alpha^{p^\nu} \in F\}$$

$K^{p^\nu}$  是  $K$  的子域， $F^{1/p^\nu}$  是  $\Omega/F$  的中间域。我们有

$$K \supseteq K^p \supseteq K^{p^2} \supseteq \dots$$

$$F \subseteq F^{1/p} \subseteq F^{1/p^2} \subseteq \dots \subseteq \Omega.$$

又约定

$$F^{1/p^\infty} = \bigcup_{v=0}^{\infty} F^{1/p^v}$$

那么  $F^{1/p^v}$  也是  $\Omega/F$  的一个中间域.

当  $p=0$  时, 我们约定,  $K^{p^v}=K$ ,  $F^{1/p^v}=F^{1/p^\infty}=F$ .

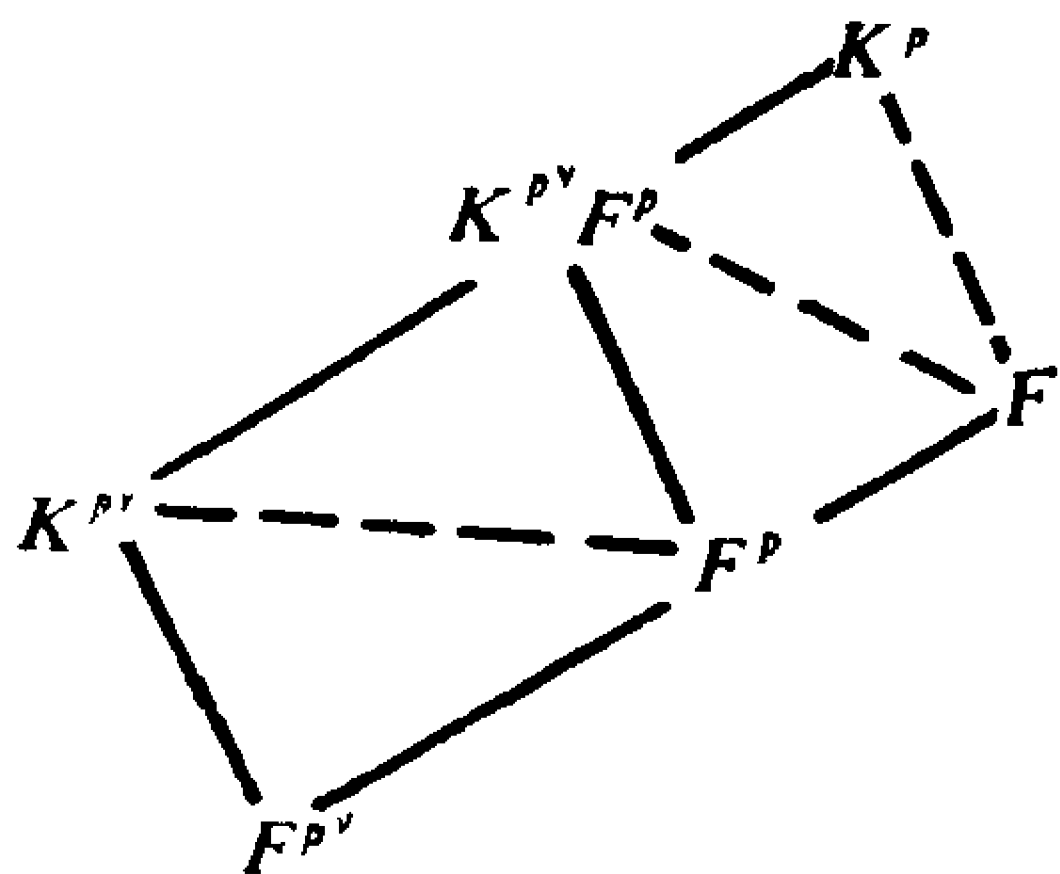
**定理 4.5.2** 设  $F$  是一个扩域,  $\text{char } F = p$ ,  $p$  是一个素数或 0.  $K$  是  $F$  的一个扩域,  $\Omega$  是  $K$  的一个代数闭包. 下列条件是等价的:

- (i)  $K/F$  是可分扩张;
- (ii)  $K^p$  与  $F$  在  $F^p$  上线性无缘;
- (iii) 对于任意非负整数  $v$ ,  $K^{p^v}$  与  $F$  在  $F^{p^v}$  上线性无缘;
- (iv) 对于  $K$  的任意扩域  $M$  和  $F$  上任意一个纯不可分的代数扩域  $L$ ,  $F \subseteq L \subseteq M$ ,  $K$  与  $L$  在  $F$  上线性无缘.
- (v)  $K$  与  $F^{1/p^\infty}$  在  $F$  上线性无缘;
- (vi) 对于任意非负整数  $v$ ,  $K$  与  $F^{1/p^v}$  在  $F$  上线性无缘.

**证** 当  $p=0$  时,  $F=F^{p^v}=F^{1/p^v}=F^{1/p^\infty}$ ,  $K^{p^v}=K$ ,  $L=F$ . 所以 (i)–(vi) 自然都是等价的. 设  $p>0$ . 我们证明 (i)–(vi) 的等价性.

(i)  $\implies$  (ii)  $\omega: \Omega \ni \xi \mapsto \xi^p \in \Omega$  是  $\Omega$  的一个自同构, 我们有  $\omega(K)=K^p$ ,  $\omega(F^{1/p})=F$ ,  $\omega(F)=F^p$ . 因为  $K$  与  $F^{1/p}$  在  $F$  上线性无缘, 所以  $\omega(K)$  与  $\omega(F^{1/p})$  在  $\omega(F)$  上线性无缘.

(ii)  $\implies$  (iii)  $v=0$  时是明显的;  $v=1$  时就是 (ii). 设  $v \geq 1$ , 并且假设  $K^{p^{v-1}}$  与  $F$  在  $F^{p^{v-1}}$  上线性无缘. 于是  $K^{p^v} = \omega(K^{p^{v-1}})$  与  $F^p = \omega(F)$  在  $F^p = \omega(F^{p^{v-1}})$  上线性无缘. 然而  $K^{p^v} \subseteq K^p$ ,  $F^p \subseteq K^p$ , 所以  $K^{p^v} F^p \subseteq K^p$ . 因为  $K^p$  与  $F$  在  $F^p$  上线性无缘, 所以  $K^{p^v} F^p$  与  $F$  也在  $F^p$  上线性无缘. 于是由 4.3.5.



$K^{p^e}$  与  $F$  在  $F^{p^e}$  上线性无缘.

(iii)  $\implies$  (iv) 设  $M$  是  $K$  的任意一个扩域,  $L$  是  $M/F$  的一个中间域且  $L/F$  是纯不可分的代数扩张. 我们证明,  $K$  与  $L$  在  $F$  上线性无缘. 为此, 只需证明, 对于  $L$  的任意一个包含  $F$  的有限次子域  $L'$ ,  $F \subseteq L' \subseteq L$ ,  $[L' : F] < \infty$ ,  $K$  与  $L'$  在

$F$  上线性无缘. 因此不妨设  $[L : F] < \infty$ . 因为  $L/F$  是有限次纯不可分扩张, 由 2.8.4, 存在一个非负整数  $e$ , 使得  $L^{p^e} \subseteq F$ . 然而由 (iii),  $K^{p^e}$  与  $F$  在  $F^{p^e}$  上线性无缘, 所以  $K^{p^e}$  与  $L^{p^e}$  在  $F^{p^e}$  上线性无缘. 考虑

$$\sigma : M^{p^e} \ni \xi^{p^e} \mapsto \xi \in M.$$

这是  $M^{p^e}$  到  $M$  内的同态单射. 显然  $\sigma(K^{p^e}) = K$ ,  $\sigma(L^{p^e}) = L$ ,  $\sigma(F^{p^e}) = F$ . 所以  $K$  与  $L$  在  $F$  上线性无缘.

(iv)  $\implies$  (v) 设  $\alpha \in F^{1/p^\infty}$ . 那么存在某一个整数  $e \geq 0$ , 使得  $\alpha \in F^{1/p^e}$ , 从而  $\alpha^{p^e} \in F$ . 于是由 2.8.2,  $F^{1/p^\infty}$  是  $F$  的一个纯不可分代数扩域, 且  $F \subseteq F^{1/p^\infty} \subseteq \Omega$ , 由 (iv),  $K$  与  $F^{1/p^\infty}$  在  $F$  上线性无缘.

(v)  $\implies$  (vi) 对于任意  $v \geq 0$ ,  $F^{1/p^v} \subseteq F^{1/p^\infty}$ .

(vi)  $\implies$  (i) 显然. ■

**推论 4.5.3** 设  $K$  是域  $F$  上的一个可分扩域,  $E$  是  $K/F$  的一个中间域. 则  $E$  是  $F$  上的可分扩域.

**证** 令  $\Omega$  是  $K$  的一个代数闭包.  $F^{1/p} = \{\alpha \in \Omega \mid \alpha^p \in F\}$ . 因为  $K/F$  可分, 所以  $K$  与  $F^{1/p}$  在  $F$  上线性无缘, 因而  $E$  与  $F^{1/p}$  在  $F$  上线性无缘. ■

**推论 4.5.4** 设  $F \subseteq E \subseteq K$  是一串扩域. 如果  $E/F$  和  $K/E$  都

是可分扩张, 则  $K/F$  也是可分扩张.

证 令  $\Omega$  是  $K$  的一个代数闭包. 那么

$$F^{1/p} = \{\alpha \in \Omega \mid \alpha^p \in F\} \subseteq E^{1/p} = \{\alpha \in \Omega \mid \alpha^p \in E\}.$$

所以  $F^{1/p}E = E(F^{1/p}) \subseteq E^{1/p}$ . 由题设,  $K$  与  $E^{1/p}$  在  $E$  上线性无缘, 所以  $K$  与  $F^{1/p}E$  在  $E$  上线性无缘. 又  $E$  与  $F^{1/p}$  在  $F$  上线性无缘. 于是由 4.3.5,  $K$  与  $F^{1/p}$  在  $F$  上线性无缘. ■

注意 如果  $K/F$  是可分扩域, 而  $E$  是  $K/F$  的一个中间域, 一般来说,  $K/E$  不一定是可分的. 参看定理 4.5.5 下面的例.

定理 4.5.5 一个域  $F$  的任意纯超越扩域  $K$  都是  $F$  上的可分扩域.

证  $\text{char } F = 0$  时是显然的. 设  $\text{char } F = p > 0$ . 令  $B$  是  $K/F$  的一个超越基.  $K = F(B)$ , 则  $K$  是整环  $R = F[B]$  的商域. 根据 4.3.3, 我们只需证明,  $R$  的一个基在  $F^{1/p}$  上线性无关.

一切关于  $B$  中有限个元素的单项式

$$M_{(i)}(x) = x_1^{i_1} \cdots x_n^{i_n}, \quad x_j \in B, i_j \geq 0 \quad (1 \leq j \leq n),$$

所组成的集是  $R$  在  $F$  上一个基. 如果有

$$\sum \alpha_{(i)} M_{(i)}(x) = 0,$$

$\sum$  是有限和,  $\alpha_{(i)} \in F^{1/p}$ , 那么

$$\sum \alpha'_{(i)} M_{(i)}(x)^p = 0,$$

$\alpha'_{(i)} \in F$ . 因为  $B$  在  $F$  上代数无关, 而  $M_{(i)}(x)^p$  是两两不同的单项式, 所以  $\alpha'_{(i)} = 0$ , 于是  $\alpha_{(i)} = 0, \quad \forall (i)$ . 这就证明了  $\{M_{(i)}(x)\}$  在  $F$  上线性无关. ■

例 设  $F$  是一个域,  $\text{char } F = 2$ ,  $t$  是  $F$  上一个超越元. 令  $\Omega$  是域  $F(t)$  的一个代数闭包,  $u \in \Omega$  是  $F(t)$  上多项式  $X^3 - (t^2 + 1)$  的一个根:  $u^3 = t^2 + 1$ . 令  $K = F(t, u) \subseteq \Omega$ . 那么  $K$  是  $F(t)$  上可分扩域; 又由 4.5.5,  $F(t)$  是  $F$  上可分扩域. 所以  $K$  是  $F$  上可分扩域.

然而另一方面, 我们有  $t^2 = u^3 - 1$ , 所以  $t$  是  $F(u)$  上多项式

$X^2 - (u^3 - 1)$ 的根. 而  $K = F(u)(t)$  是  $F(u)$  的纯不可分扩域.

最后再给出关于完备域的一个进一步的性质. 回忆在 2.9 中的定义. 一个域称为完备的, 如果它的任何代数扩域都是可分的. 现在我们证明, “代数”这个限制可以去掉.

**定理 4.5.6** 一个域是完备的必要且只要它的任意扩域都是可分的.

**证** 设  $F$  是一个域.  $\text{char } F = 0$  的情形是显然的. 设  $\text{char } F = p > 0$ .

设  $F$  是完备的. 则  $F = F^p$ . 令  $K$  是  $F$  的任意一个扩域, 则  $K^p$  与  $F$  在  $F = F^p$  上线性无缘, 因而由 4.5.2,  $K/F$  是可分扩张.

反之显然. ■

## 习 题

1. 设  $K$  是域  $F$  的一个扩域. 证明,  $K$  在  $F$  上可分必要且只要对于  $K$  中任意有限个元素  $\alpha_1, \dots, \alpha_n$  来说,  $F(\alpha_1, \dots, \alpha_n)$  在  $F$  上可分.

2. 设  $F$  是一个域,  $\text{char } F = p$ , 这里  $p$  或者是素数, 或者等于零,  $M$  是  $F$  的一个扩域. 对于  $M$  的元素  $\alpha$  和整数  $\nu \geq 0$ , 当  $p > 0$  时,  $\alpha^{p^\nu}$  表示通常的  $\alpha$  的  $p^\nu$  次幂, 当  $p = 0$  时, 约定  $\alpha^{p^\nu} = \alpha$ . 令

$$M_i = \{\alpha \in M \mid \alpha^{p^\nu} \in F \text{ 对某一 } \nu \geq 0\}.$$

证明.  $M_i$  是  $M/F$  的一个中间域, 它是  $M$  中在  $F$  上纯不可分元素的全体.  $M_i$  称为  $F$  在  $F$  中的纯不可分闭包.

3. 设  $K$  是域  $F$  的一个扩域. 证明, 下列四个条件等价:

(i)  $K$  是  $F$  上的可分扩域;

(ii) 对于  $K$  的任意扩域  $M$ , 令  $M_i$  是  $F$  在  $M$  中的纯不可分闭包, 则  $M_i$  与  $K$  在  $F$  上线性无缘;

(iii) 设  $M$  是  $F$  的任意扩域,  $L$  是  $M/F$  的中间域, 且  $L$  是

$F$  上一个纯不可分 (代数) 扩域, 则  $K$  与  $L$  在  $F$  上线性无缘;

(iv) 设  $\Omega$  是  $K$  的一个代数闭包,  $\Omega_i$  是  $F$  在  $\Omega$  内的纯不可分闭包, 则  $\Omega_i$  与  $K$  在  $F$  上线性无缘.

4. 设  $F$  是一个特征为  $p > 0$  的域. 证明, 域扩张  $K/F$  是可分的必要且只要对于  $K$  中任意一组在  $F$  上线性无关的元素  $u_1, \dots, u_n$  来说,  $u_1^p, \dots, u_n^p$  也在  $F$  上线性无关.

#### 4.6 可分生成的扩域

设  $K$  是域  $F$  的一个扩域.  $K$  在  $F$  上一个超越基  $B$  说是可分的, 如果  $K$  是  $F(B)$  上可分 (代数) 扩域.  $K$  叫做域  $F$  上的一个可分生成的扩域, 如果存在  $K$  在  $F$  上一个可分超越基  $B$ , 使得  $K$  是  $F(B)$  上一个可分 (代数) 扩域.

**定理 4.6.1** 设  $F$  是一个域.

(i)  $F$  上可分生成的扩域都是可分扩域.

(ii)  $F$  上有限生成的可分扩域都是可分生成的扩域.

**证** (i) 设  $K$  是  $F$  上一个可分生成的扩域. 那么存在  $K/F$  的一个可分超越基  $B$ , 使得  $K$  是  $F(B)$  上可分扩域. 又由 4.5.5,  $F(B)$  是  $F$  上可分扩域. 所以  $K$  是  $F$  上可分扩域.

(ii) 设  $K = F(\alpha_1, \dots, \alpha_n)$  是  $F$  上一个可分扩域. 我们证明, 在  $\{\alpha_1, \dots, \alpha_n\}$  中可以选出  $K/F$  的一个可分超越基.

如果  $\text{char } F = 0$ , 那么由 4.1.4, 在  $\{\alpha_1, \dots, \alpha_n\}$  中可以选出  $K/F$  的一个超越基, 这时  $K/F$  的任意一个超越基自然都是可分的.

现在设  $\text{char } F = p > 0$ . 我们对  $n$  作归纳法.  $n = 0$  时,  $K = F$ ,  $B = \emptyset$ , 论断(ii)显然成立. 假设对于  $F$  上任意一个由  $n-1$  个元素生成的可分扩域  $E = F(\beta_1, \dots, \beta_{n-1})$  来说, 可以在  $\{\beta_1, \dots, \beta_{n-1}\}$  中选取一个可分超越基. 令  $K = F(\alpha_1, \dots, \alpha_n)$  是  $F$  上一个可分扩域. 如果  $\alpha_1, \dots, \alpha_n$  在  $F$  上代数无关, 那么  $\{\alpha_1, \dots,$



$\alpha_n\}$ 就是 $K/F$ 的一个可分超越基. 设 $\alpha_1, \dots, \alpha_n$ 在 $F$ 上代数相关, 适当编号, 可设 $\alpha_1, \dots, \alpha_r$  ( $0 \leq r < n$ )是 $K/F$ 的一个超越基. 那么 $\alpha_1, \dots, \alpha_{r+1}$ 在 $F$ 上代数相关. 于是存在非零多项式 $f(X_1, \dots, X_{r+1}) \in F[X_1, \dots, X_{r+1}]$ , 使得

$$f(\alpha_1, \dots, \alpha_{r+1}) = 0.$$

不妨设 $f \in F[X_1, \dots, X_{r+1}]$ 是满足这一条件的非零多项式中次数最低的一个. 则 $f(X_1, \dots, X_{r+1})$ 不可约. 我们断言, 不存在 $g \in F[X_1, \dots, X_{r+1}]$ , 使得

$$f(X_1, \dots, X_{r+1}) = g(X_1^p, \dots, X_{r+1}^p).$$

事实上, 如果有

$$g = \sum a_{(i)} X_1^{i_1} \cdots X_{r+1}^{i_{r+1}} \in F[X_1, \dots, X_{r+1}],$$

$a_{(i)} \in F$ , 使得

$$f(X_1, \dots, X_{r+1}) = \sum a_{(i)} X_1^{p i_1} \cdots X_{r+1}^{p i_{r+1}},$$

令

$$\begin{aligned} h(X_1, \dots, X_{r+1}) &= \sum a_{(i)}^{1/p} X_1^{i_1} \cdots X_{r+1}^{i_{r+1}} \in \\ &\in F^{1/p}[X_1, \dots, X_{r+1}], \end{aligned}$$

则 $h(\alpha_1, \dots, \alpha_{r+1})^p = f(\alpha_1, \dots, \alpha_{r+1}) = 0$ .  $\deg h < \deg f$ .

令 $\{M_{(i)}(X) = X_1^{i_1} \cdots X_{r+1}^{i_{r+1}}\}$ 是出现在 $h(X_1, \dots, X_{r+1})$ 中一切单项式的集, 令 $M_{(i)}(\alpha) = \alpha_1^{i_1} \cdots \alpha_{r+1}^{i_{r+1}}$ , 则 $\{M_{(i)}(\alpha)\}$ 在 $F^{1/p}$ 上线性相关. 然而根据题设,  $K$ 与 $F^{1/p}$ 在 $F$ 上线性无缘, 因此单项式集 $\{M_{(i)}(\alpha)\}$ 也必须在 $F$ 上线性相关. 于是有线性关系

$$\sum b_{(i)} M_{(i)}(\alpha) = \sum b_{(i)} \alpha_1^{i_1} \cdots \alpha_{r+1}^{i_{r+1}} = 0,$$

$b_{(i)} \in F$ , 且 $b_{(i)}$ 不全为零. 令

$$u(X_1, \dots, X_{r+1}) = \sum b_{(i)} X_1^{i_1} \cdots X_{r+1}^{i_{r+1}}.$$

则 $u \in F[X_1, \dots, X_{r+1}]$ ,  $u \neq 0$  且 $u(\alpha_1, \dots, \alpha_{r+1}) = 0$ . 然而 $\deg u < \deg f$ , 这与 $f$ 的取法矛盾.

这样, 一定有某一个 $X_i$  ( $1 \leq i \leq r+1$ ),  $X_i$ 在 $f$ 中出现, 但不以 $p$ 次幂出现. 不妨设 $i=1$ . 于是 $f(X_1, \alpha_2, \dots, \alpha_{r+1})$ 作为

$F(\alpha_2, \dots, \alpha_{r+1})$  上关于  $X_1$  的多项式, 是可分的. 然而  $f(\alpha_1, \alpha_2, \dots, \alpha_{r+1}) = 0$ , 所以  $\alpha_1$  是  $F(\alpha_2, \dots, \alpha_{r+1})$  上的可分元素, 因而是  $E = F(\alpha_2, \dots, \alpha_n)$  上的可分元素.

我们有  $F \subseteq E \subseteq K$ . 因为  $K/F$  是可分的, 所以由 4.5.3,  $E/F$  是可分的, 于是由归纳法的假设, 在  $\{\alpha_2, \dots, \alpha_n\}$  中可以选出  $E/F$  的一个可分超越基  $B$ .  $E$  是  $F(B)$  上可分代数扩域, 而  $K = E(\alpha_1)$  是  $E$  上可分代数扩域, 所以  $K$  是  $F(B)$  上可分代数扩域, 而  $B$  是  $K/F$  的一个可分超越基. ■

由定理 4.6.1 的证明可以直接得出以下两个推论.

**推论 4.6.2** 设  $K = F(\alpha_1, \dots, \alpha_n)$  是域  $F$  的一个有限生成的可分扩域, 那么在  $\{\alpha_1, \dots, \alpha_n\}$  中可以选出  $K/F$  的一个可分超越基. ■

**推论 4.6.3** 设  $F$  是一个完备域,  $K$  是  $F$  上一个有限生成的扩域. 则  $K$  是  $F$  上可分生成的扩域. ■

下面的两个例子告诉我们, 一个域  $F$  上的可分扩域不一定是可分生成的; 即使是可分生成的, 也不一定每一个超越基都是可分的.

**例 1** 设  $F$  是一个特征为  $p > 0$  的域.  $K = F(t)$ ,  $t$  是  $F$  上一个超越元.  $K$  自然是  $F$  上可分生成的扩域,  $\{t\}$  就是  $K/F$  的一个可分超越基. 然而  $\{t^p\}$  也是  $K/F$  的一个超越基, 但是  $K/F(t^p)$  是纯不可分扩张.

**例 2** 设  $F$  是一个特征为  $p > 0$  的完备域.  $E = F(t)$ ,  $t$  是  $F$  上一个超越元. 令  $\Omega$  是  $E$  的一个代数闭包. 多项式  $X^{p^{-1}} - t \in E[X]$  的根是  $t^{p^{-1}}$ , 令  $K = F(t, t^{p^{-1}}, t^{p^{-2}}, \dots) = \bigcup_{v \geq 1} F(t^{p^{-v}}) \subseteq \Omega$ . 因为

$E$  是完备域, 所以由 4.5.6,  $K$  是  $F$  上可分扩域.

然而  $K/F$  不是可分生成的. 事实上,  $\text{tr.deg}_F K = 1$ . 假设  $\{u\}$  是  $K/F$  的一个可分超越基. 那么存在一个整数  $e \geq 1$ , 使得

$$F(u) \subseteq F(t, t^{p^{-1}}, \dots, t^{p^{-e}}) = F(t^{p^{-e}}) = E(t^{p^{-e}}) = K'.$$

对于任意整数  $v \geq e+1$ , 令

$$K'_v = F(t, t^{p^{-1}}, \dots, t^{p^{-v}}) = E(t^{p^{-v}}).$$

因为  $K/F(u)$  是可分代数扩张, 而  $F(u) \subseteq K' \subseteq K'_v \subseteq K$ , 所以  $K'_v/K'$  是可分代数扩张, 另一方面, 多项式  $X^{p^v} - t \in E[X]$  是不可约的 (利用 Eisenstein 判别法很容易看出), 所以  $[K'_v : E] = p^v$ , 从而  $[K'_v : K'] = p^{v-e} > 1$ . 因此  $K'_v/K'$  是纯不可分扩张. 这就导致矛盾.

**定理 4.6.4** 设  $K$  和  $L$  都是域  $F$  的扩域, 并且被包含在某一个共同的扩域  $M$  内.  $K/F$  是可分扩张, 并且  $K$  与  $L$  在  $F$  上代数无关. 那么合成域  $KL$  是  $L$  上的可分扩域.

**证** 首先注意,  $KL = L(K)$  的每一个元素都可以表示成

$$f(\alpha_1, \dots, \alpha_m)/g(\alpha_1, \dots, \alpha_m),$$

$$f, g \in L[X_1, \dots, X_m], g(\alpha_1, \dots, \alpha_m) \neq 0,$$

的形式. 因此  $KL$  的任意一个在  $L$  上有限生成的子域都包含在一个合成域  $K'L$  内. 这里  $K' \subseteq K$  并且是  $F$  上有限生成的. 由 4.5.3,  $K'/F$  是可分的. 这样, 不失一般性, 我们可以假设  $K$  是  $F$  上有限生成的.

设  $K$  是  $F$  上一个有限生成的可分扩域. 由 4.6.1,  $K$  是  $F$  上可分生成扩域. 令  $\{t_1, \dots, t_n\}$  是  $K$  在  $F$  上一个可分超越基, 令  $E = F(t_1, \dots, t_n)$ . 则  $K/E$  是可分代数扩张. 由题设,  $t_1, \dots, t_n$  在  $L$  上代数无关, 所以  $\{t_1, \dots, t_n\}$  也是  $KL = L(K)$  在  $L$  上一个超越基. 在  $KL$  中,  $K$  的每一个元素在  $E = F(t_1, \dots, t_n)$  上是可分代数元, 因而也是  $EL = L(t_1, \dots, t_n)$  上的可分代数元. 由此  $KL$  是  $L(t_1, \dots, t_n)$  上可分代数扩域,  $\{t_1, \dots, t_n\}$  是  $K/L$  的一个可分超越基, 这样,  $KL$  是  $L$  上可分生成的扩域, 因而是可分扩域. ■

## 习 题

1. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域, 并且  $K$  和  $L$  都是  $F$  上可分扩域. 如果  $K$  与  $L$  在  $F$  上代数无关, 则  $KL$  是  $F$  上可分扩域.

2. 设  $K$  和  $L$  都是域扩张  $M/F$  的中间域, 且  $K$  与  $L$  在  $F$  上线性无缘. 证明,  $K/F$  可分必要且只要  $KL/L$  可分.

3. 设  $F$  是一个特征为  $p > 0$  的完备域,  $K$  是  $F$  上一个非完备扩域, 又  $\text{tr.deg}_F K = 1$ . 证明,  $K$  是  $F$  上可分生成的.

4. 设  $F_0$  是一个特征为  $p > 0$  的域,  $x, y, z$  是  $F_0$  上代数无关的元素. 令  $K = F_0(x, y, z, u)$ ,  $u^p = xy^p + y$ . 证明:

(i)  $F = F_0(x, y)$  在  $K$  中是代数闭的;

(ii)  $K/F$  不是可分生成的.

## 4.7 导 子

在这一章的最后一节, 我们介绍一下导子的概念. 导子是通常导数概念的自然推广, 它在域论和代数的其它一些分支中都占有一定的重要地位.

设  $R$  是一个有单位元  $1$  的交换环,  $A$  是  $R$  的一个子环, 并且  $A$  含有  $R$  的单位元. 在这一节里, 说到  $R$  和  $A$ , 都作这样理解.

$A$  到  $R$  的一个映射  $D: A \rightarrow R$  叫做  $A$  到  $R$  的一个导子, 如果下列两个条件被满足:

$$(1) \quad D(a+b) = D(a) + D(b);$$

$$(2) \quad D(ab) = aD(b) + bD(a),$$

这里  $a, b$  是  $A$  的任意元素.

环  $R$  到  $R$  的导子叫做  $R$  的导子.

例 1 设  $R = F[X_1, \dots, X_n]$  是某一个域  $F$  上  $n$  元多项式环. 对于每一个  $X_i$  和  $f \in R$ , 令  $\partial f / \partial X_i$  表示  $f$  关于  $X_i$  的偏导数, 也

就是将  $f$  看成整环  $F[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$  上关于  $X_i$  的一元多项式对  $X_i$  的导数。那么

$$\partial/\partial X_i : R \ni f \mapsto \partial f/\partial X_i \in R$$

是  $R$  的导子。

**定理 4.7.1** 设  $D : A \rightarrow R$  是  $A$  到  $R$  的一个导子。则

- (i)  $D(1) = 0$ ,  $D(0) = 0$ ,  $D(-a) = -D(a)$ ,  $\forall a \in A$ ;
- (ii)  $S = \{a \in A \mid D(a) = 0\}$  作成  $A$  的一个子环;
- (iii)  $D(a^n) = na^{n-1}D(a)$ ,  $a \in A$ ,  $n$  是任意正整数;
- (iv) 对于  $a, b \in A$ , 且  $b$  是一个可逆元素,

$$D(a/b) = (bD(a) - aD(b))/b^2.$$

**证** (i) 由(2),  $D(1) = D(1^2) = D(1) + D(1) \implies D(1) = 0$ .

由(1),  $D(0) = D(0+0) = D(0) + D(0) \implies D(0) = 0$ . 于是,

$$D(a) + D(-a) = D(a + (-a)) = D(0) = 0.$$

$$\implies D(-a) = -D(a).$$

(ii) 由(i)及(2), 对于  $a, b \in S$ , 我们有  $a-b \in S$ ,  $ab \in S$ .

所以  $S$  是  $A$  的子环。

(iii) 由(2), 对  $n$  作归纳法。

(iv) 设  $b$  是  $A$  的一个可逆元素。那么

$$0 = D(1) = D(bb^{-1}) = bD(b^{-1}) + b^{-1}D(b).$$

所以,  $D(b^{-1}) = -b^{-2}D(b)$ . 于是

$$D(a/b) = D(ab^{-1}) = aD(b^{-1}) + b^{-1}D(a)$$

$$= -ab^{-2}D(b) + b^{-1}D(a) = b^{-2}(bD(a) - aD(b)).$$

设  $B$  是  $R$  的一个子环, 且  $A \subseteq B \subseteq R$ . 令  $D$  是  $A$  到  $R$  的一个导子。如果  $\tilde{D} : R \rightarrow R$  是  $B$  到  $R$  的一个导子, 且  $\tilde{D}|_A = D$ , 那么就说  $\tilde{D}$  是  $D$  在  $B$  上一个开拓。

把  $A$  的每一个元素都映成零元的零映射显然是  $A$  的一个导子, 称为平凡导子。设  $D : R \rightarrow R$  是  $R$  的一个导子,  $A$  是  $R$  的一个子环。如果  $D|_A$  是  $A$  的平凡导子, 那么就说  $D$  在  $A$  上是平凡的,

或者说  $D$  是  $A$  上的导子. 这时  $D$  是  $R$  的一个  $A$ -线性映射, 因为对于  $a \in A, \alpha \in R$ , 都有  $D(a\alpha) = aD(\alpha)$ .

设  $F$  是一个域,  $F_0$  是  $F$  的素域. 那么或者  $F_0 \cong \mathbb{Q}$ , 或者  $F_0 \cong F_p$ . 由 4.7.1 容易看出,  $F$  的每一个导子都是在  $F_0$  上平凡的.

**例 2** 设  $D$  是环  $R$  的一个导子. 令  $P = R[X_1, \dots, X_n]$  是  $R$  上  $n$  元多项式环. 则  $D$  可以看成  $R$  到  $P$  的一个导子. 对于

$$f = \sum_{(i) = (i_1, \dots, i_n)} a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \in P.$$

定义

$$f^D = \sum_{(i)} D(a_{(i)}) X_1^{i_1} \cdots X_n^{i_n}.$$

那么映射  $P \ni f \mapsto f^D \in P$  是  $P$  的一个导子, 它是  $D$  在  $P$  上的一个开拓.

现在设  $R$  是一个整环,  $F$  是  $R$  的商域.  $R$  的导子可以看成  $R$  到  $F$  的导子. 我们看  $R$  的导子在  $F$  上的开拓.

**定理 4.7.2** 设  $R$  是一个整环,  $F$  是  $R$  的商域.  $R$  的每一个导子  $D$  都可以唯一地开拓为  $F$  的一个导子  $\tilde{D}$ ; 对于  $a, b \in R, b \neq 0$ ,

$$\tilde{D}(a/b) = (bD(a) - aD(b))/b^2.$$

**证** 如果  $a/b = a'/b'$ ,  $a, a', b, b' \in R$ , 则  $ab' = a'b$ . 于是

$$aD(b') + b'D(a) = a'D(b) + bD(a'),$$

从而

$$b'(D(a) - (a'/b')D(b)) = b(D(a') - (a/b)D(b')).$$

因为  $a/b = a'/b'$ , 所以

$$(D(a) - (a/b)D(b))/b = (D(a') - (a'/b')D(b'))/b',$$

即

$$(bD(a) - aD(b))/b^2 = (b'D(a') - a'D(b'))/b'^2.$$

这样, 定义

$$\tilde{D}(a/b) = (bD(a) - aD(b))/b^2$$

不依赖于  $a/b$  的表示法, 所以  $\tilde{D}: F \rightarrow F$  是一个映射. 直接验证可知条件(1), (2)都被满足, 所以  $\tilde{D}$  是  $F$  的一个导子, 并且是  $D$

在  $F$  上的开拓.

设  $D'$  也是  $D$  在  $F$  上一个开拓. 那么由 4.7.1 (iv), 必须有

$$\begin{aligned} D'(a/b) &= (bD'(a) - aD'(b))/b^2 \\ &= (bD(a) - aD(b))/b^2 = \bar{D}(a/b). \end{aligned}$$

现在设  $F$  是一个域.  $K = F(\alpha_1, \dots, \alpha_n)$  是  $\alpha_1, \dots, \alpha_n$  在  $F$  上所生成的扩域. 我们考虑  $F$  的导子在  $K$  上的开拓.

令  $F[X_1, \dots, X_n]$  是  $F$  上  $n$  元多项式环. 我们以下把它简记作  $F[X]$ . 对于  $f \in F[X]$ , 我们将  $f(\alpha_1, \dots, \alpha_n)$  简记作  $f(\alpha)$  并且记

$$\left( \frac{\partial f}{\partial X_i} \right)_\alpha = \frac{\partial f}{\partial X_i}(\alpha_1, \dots, \alpha_n).$$

设  $D$  是  $F$  的一个导子. 我们问, 是否存在  $K$  的导子  $\bar{D}$ , 使得  $\bar{D}$  是  $D$  的开拓? 如果  $\bar{D} : K \rightarrow K$  是这样一个开拓, 那么对于任意  $f \in F[X]$  且  $f(\alpha) = 0$ , 以下等式成立:

$$(3) \quad f^D(\alpha) + \sum_{i=1}^n \left( \frac{\partial f}{\partial X_i} \right)_\alpha \bar{D}(\alpha_i) = \bar{D}(f(\alpha)) = 0,$$

这里  $f^D$  的意义如例 2. 令

$$I = \{f \in F[X] \mid f(\alpha) = 0\}.$$

则  $I$  是  $F[X]$  的一个理想, 叫做  $(\alpha) = (\alpha_1, \dots, \alpha_n)$  在  $F[X]$  内所确定的理想. 令  $\{f_\lambda\}_{\lambda \in \Lambda}$  是  $I$  的一组生成元<sup>1)</sup>. 那么  $I$  的每一个元素  $f$  都可以写成  $f = \sum_{\lambda} g_\lambda f_\lambda$  (有限和),  $g_\lambda \in F[X]$ . 因此根据导子的定义容易证明, 如果每一个生成元  $f_\lambda (\lambda \in \Lambda)$  都满足关系式(3), 则  $I$  中每一个多项式  $f$  也满足关系式(3).

下面的定理告诉我们, 关系式(3)也是导子  $\bar{D}$  存在的充分条件.

1) 在下一章里将会看到,  $F[X]$  的任意理想都可以由有限个元素生成(参看 5.2.5).

定理 4.7.3 设  $K = F(\alpha_1, \dots, \alpha_n)$  是  $\alpha_1, \dots, \alpha_n$  在  $F$  上所生成的扩域,  $D$  是  $F$  的一个导子. 令

$$I = \{f \in F[X] \mid f(\alpha) = 0\}$$

是  $(\alpha) = (\alpha_1, \dots, \alpha_n)$  在  $F[X]$  内所确定的理想,  $\{f_\lambda\}_{\lambda \in \Lambda}$  是  $I$  的一组生成元. 如果  $u_1, \dots, u_n \in K$ , 满足以下的一组关系:

$$f_\lambda^D(\alpha) + \sum_{i=1}^n \left( \frac{\partial f_\lambda}{\partial X_i} \right)_\alpha u_i = 0, \quad \forall \lambda \in \Lambda,$$

那么存在  $K$  的导子  $\tilde{D}$ , 使得  $\tilde{D}|_F = D$ , 并且  $\tilde{D}(\alpha_i) = u_i, 1 \leq i \leq n$ .

证 设  $f \in I$ , 则  $f = \sum_{\lambda \in \Lambda} g_\lambda f_\lambda$  (有限和). 因为  $f_\lambda(\alpha) = 0$ , 所以

$$f^D(\alpha) = \sum_{\lambda \in \Lambda} g_\lambda(\alpha) f_\lambda^D(\alpha),$$

$$\left( \frac{\partial f}{\partial X_i} \right)_\alpha = \sum_{\lambda \in \Lambda} g_\lambda(\alpha) \left( \frac{\partial f_\lambda}{\partial X_i} \right)_\alpha, \quad 1 \leq i \leq n.$$

于是由题设的条件, 我们有

$$f^D(\alpha) + \sum_{i=1}^n \left( \frac{\partial f}{\partial X_i} \right)_\alpha u_i = 0.$$

令  $R = F[\alpha_1, \dots, \alpha_n] = \{f(\alpha) \mid f(X) \in F[X]\}$ . 则  $R$  是一个整环, 并且  $K$  是  $R$  的商域. 设  $f(X), g(X) \in F[X]$ . 如果  $f(\alpha) = g(\alpha)$ , 则  $f - g \in I$ . 于是

$$f^D(\alpha) + \sum_{i=1}^n \left( \frac{\partial f}{\partial X_i} \right)_\alpha u_i = g^D(\alpha) + \sum_{i=1}^n \left( \frac{\partial f}{\partial X_i} \right)_\alpha u_i.$$

对于任意  $v \in R$ , 则有  $f(X) \in F[X]$ , 使得  $v = f(\alpha)$ . 我们定义

$$D'(v) = f^D(\alpha) + \sum_{i=1}^n \left( \frac{\partial f}{\partial X_i} \right)_\alpha u_i.$$

则  $D'(v)$  不依赖于  $f(X)$  的选取. 因而  $v \mapsto D'(v)$  是  $R$  到  $K$  的一个映射. 易证  $D'$  是一个导子, 且  $D'(\alpha_i) = u_i, 1 \leq i \leq n$ . 由 4.7.2,



$D'$  可以唯一地开拓为  $K$  的导子  $\tilde{D}$ .

设  $f_1, \dots, f_m \in F[X_1, \dots, X_n]$ ,  $m \times n$  矩阵

$$J(f_1, \dots, f_m) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \dots & \frac{\partial f_1}{\partial X_n} \\ \dots & \dots & \dots \\ \frac{\partial f_m}{\partial X_1} & \dots & \frac{\partial f_m}{\partial X_n} \end{pmatrix}$$

叫做  $f_1, \dots, f_m$  的 Jacobi 矩阵. 记

$$J(f_1, \dots, f_m)_a = \begin{pmatrix} \left(\frac{\partial f_1}{\partial X_1}\right)_a & \dots & \left(\frac{\partial f_1}{\partial X_n}\right)_a \\ \dots & \dots & \dots \\ \left(\frac{\partial f_m}{\partial X_1}\right)_a & \dots & \left(\frac{\partial f_m}{\partial X_n}\right)_a \end{pmatrix}.$$

由 4.7.3, 我们立即得到以下

**推论 4.7.4** 记号同 4.7.3. 如果  $I$  由  $n$  个多项式  $f_1, \dots, f_m \in F[X]$  生成, 那么  $D$  在  $K$  上一切开拓与线性方程组

$$J(f_1, \dots, f_m)_a \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = - \begin{pmatrix} f_1^D(\alpha) \\ \vdots \\ f_m^D(\alpha) \end{pmatrix}$$

在  $K$  内的一切解之间存在着 1-1 对应.

现在考虑  $K = F(\alpha)$  是域  $F$  的单扩域的情形. 我们有

**定理 4.7.5** 设  $K = F(\alpha)$  是域  $F$  的一个单扩域,  $D$  是  $F$  的一个导子.

(i) 如果  $\alpha$  是  $F$  上的超越元, 那么对于任意  $\gamma \in K$ , 存在  $D$  在  $K$  上的开拓  $\tilde{D}$ , 使得  $\tilde{D}(\alpha) = \gamma$ .

(ii) 如果  $\alpha$  是  $F$  上可分代数元, 那么  $D$  可以唯一地开拓为  $K$  的导子  $\tilde{D}$ .

(iii) 设  $\text{char } F = p > 0$ ,  $\alpha$  是  $F$  上不可分元素. 令  $f(X)$

是  $\alpha$  在  $F$  上的最小多项式. 那么  $D$  可以开拓为  $K$  的导子的充分且必要条件是  $f^D(\alpha) = 0$ . 如果这个条件成立, 那么对于任意  $\gamma \in K$ , 存在  $D$  在  $K$  上的开拓  $\tilde{D}$ , 使得  $\tilde{D}(\alpha) = \gamma$ .

**证** 令  $I = \{f \in F[X] \mid f(\alpha) = 0\}$  是  $\alpha$  在一元多项式环  $F[X]$  内所确定的理想.

(i) 如果  $\alpha$  是  $F$  上超越元, 则  $I = (0)$ . 这时定理 4.7.3 的条件自然被满足.

(ii) 令  $f(X)$  是  $\alpha$  在  $F$  上的最小多项式. 则  $I = (f)$ . 这时  $\partial f / \partial X = f'(X)$ . 因为  $f(X)$  是可分的, 所以  $f'(\alpha) \neq 0$ . 定理 4.7.3 的条件为  $f^D(\alpha) + f'(\alpha)u = 0$ . 从而  $u = -f^D(\alpha)/f'(\alpha)$  是唯一确定的. 所以  $D$  可以唯一地开拓为  $K$  的导子  $\tilde{D}$ ,  $\tilde{D}(\alpha) = u$ .

(iii) 因为  $\alpha$  是  $F$  上不可分元素, 所以  $f'(X) = 0$ .

如果  $D$  可以开拓为  $\tilde{D}: K \rightarrow K$ , 则

$$f^D(\alpha) + f'(\alpha)\tilde{D}(\alpha) = 0.$$

所以  $f^D(\alpha) = 0$ .

反之, 设  $f^D(\alpha) = 0$ . 那么对于任意  $\gamma \in K$ , 都有  $f^D(\alpha) + f'(\alpha)\gamma = 0$ , 由 4.7.3, 存在  $K$  的导子  $\tilde{D}$ ,  $\tilde{D}|_F = D$  且  $\tilde{D}(\alpha) = \gamma$ . ■

**推论 4.7.6** 设  $K = F(\alpha)$  是域  $F$  的一个单扩域,  $\text{char } F = p > 0$ , 且  $\alpha^p \in F$ . 令  $D$  是  $F$  的一个导子.  $D$  可以开拓为  $K$  的导子必要且只要  $D(\alpha^p) = 0$ .

如果这个条件被满足, 则对于任意  $\gamma \in K$ , 存在  $D$  在  $K$  上的开拓  $\tilde{D}$ , 使得  $\tilde{D}(\alpha) = \gamma$ .

**证** 可设  $\alpha \notin F$ . 则  $\alpha$  在  $F$  上的最小多项式是  $f(X) = X^p - a$ ,  $a = \alpha^p \in F$ , 于是

$$f^D(X) = D(1)X^p - D(a) = -D(a).$$

由定理 4.7.4 (iii), 就得到这个推论. ■

**推论 4.7.7** 设  $K = F(\alpha)$  是域  $F$  的一个单扩域,  $\gamma \in K$ .

(i) 如果  $K/F$  是超越扩张或者是不可分的代数扩域, 那么存在  $K$  在  $F$  上的导子  $D$ , 使得  $D(\alpha) = \gamma$ .

(ii) 如果  $K/F$  是可分的代数扩张, 那么  $K$  的任意在  $F$  上的导子都是  $K$  的平凡导子. ■

**定理 4.7.8** 设  $K$  是域  $F$  的一个扩域,  $D$  是  $F$  的一个导子.

(i) 如果  $\text{char} F = 0$ , 那么  $D$  一定可以开拓为  $K$  的一个导子. 这时, 对于  $K$  的一个在  $F$  上的超越元  $z$  和任意  $\gamma \in K$ , 总存在  $D$  在  $K$  上的一个开拓  $\tilde{D}$ , 使得  $\tilde{D}(z) = \gamma$ .

(ii) 如果  $\text{char} F = p > 0$  且  $F \supseteq K^p$ .  $D$  可以开拓为  $K$  的导子必要且只要  $D(K^p) = 0$ . 这时, 对给定  $\beta \in K$ ,  $\beta \notin F$  和任意  $\gamma \in K$ , 总存在  $D$  上的开拓  $\tilde{D}$ , 使得  $\tilde{D}(\beta) = \gamma$ .

**证** 考虑这样的对  $(K', D')$ , 其中  $K'$  是  $K/F$  的一个中间域,  $D' : K' \rightarrow K$  是  $K'$  到  $K$  的导子且  $D'|_F = D$ . 令  $M$  是一切这样的对  $(K', D')$  所成的集. 显然  $(F, D) \in M$ , 所以  $M \neq \emptyset$ . 对于  $(K_1, D_1)$ ,  $(K_2, D_2) \in M$ , 规定

$$(K_1, D_1) < (K_2, D_2) \iff K_1 \subseteq K_2, \text{ 且 } D_2|_{K_1} = D_1.$$

则  $M$  对于 “ $<$ ” 作成是一个偏序集. 令  $\{(K_\lambda, D_\lambda) \mid \lambda \in \Lambda\}$  是  $M$  中一个链. 令  $K' = \bigcup_{\lambda \in \Lambda} K_\lambda$ , 则  $F \subseteq K' \subseteq K$ . 设  $\alpha' \in K'$ , 那么一定有某

$\lambda \in \Lambda$ , 使  $\alpha' \in K_\lambda$ . 定义  $D'(\alpha') = D_\lambda(\alpha')$ . 容易看出,  $D'(\alpha)$  不依赖于  $\alpha'$  所在的域  $K_\lambda$  的选取, 并且  $D'$  是  $K'$  到  $K$  的一个导子, 且  $D'|_F = D$ , 所以  $(K', D') \in M$ , 并且是  $\{(K_\lambda, D_\lambda) \mid \lambda \in \Lambda\}$  的一个上界. 于是由 Zorn 引理,  $M$  有一个极大元素  $(L, \tilde{D})$ . 我们证明,  $L = K$ .

(i) 设  $\text{char} F = 0$ , 如果  $L \subsetneq K$ , 那么存在  $\alpha \in K$ , 但  $\alpha \notin L$ , 于是  $L \subsetneq L(\alpha) \subseteq K$ . 因为  $\text{char} F = 0$ , 所以不论  $\alpha$  是  $F$  上的代数元 (因而是可分代数元) 还是超越元, 由定理 4.7.5,  $\tilde{D}$

都可以开拓为  $L(\alpha)$  的导子  $D^*$ . 从而  $(L(\alpha), D^*) \in M$ . 这与  $(L, \tilde{D})$  的极大性矛盾. 这样, 必须  $L = K$ ,  $\tilde{D} : K \rightarrow K$  是  $D$  在  $K$  上的开拓.

设  $z \in K$  是  $F$  上一个超越元, 那么由 4.7.5, 对于任意  $\gamma \in K$ , 存在  $D$  在  $F(z)$  上的开拓  $\tilde{D}$ , 使得  $\tilde{D}(\alpha) = \gamma$ . 于是由上面的证明, 对于域  $F(z)$  和  $F(z)$  的导子  $\tilde{D}$ , 存在  $\bar{D}$  在  $K$  上的开拓  $\tilde{D}$ ,  $\tilde{D}|_{F(z)} = \tilde{D}$ , 所以  $\tilde{D}|_F = D$ , 且  $\tilde{D}(z) = \gamma$ .

(ii) 设  $\text{char } F = p > 0$ .  $K^p = \{\alpha = \alpha^p \mid \alpha \in K\} \subseteq F$ . 如果  $D$  可以开拓为  $K$  的导子  $\tilde{D}$ , 那么对于  $\alpha = \alpha^p \in K^p \subseteq F$ ,

$$D(\alpha) = \tilde{D}(\alpha) = \tilde{D}(\alpha^p) = p\alpha^{p-1}\tilde{D}(\alpha) = 0.$$

所以  $D(K^p) = 0$ .

反之, 设  $(L, \tilde{D})$  是上述的  $M$  中的极大元. 如果  $L \subsetneq K$ , 则存在  $\alpha \in K, \alpha \notin L$ , 于是  $L \subsetneq L(\alpha) \subseteq K$ .  $\alpha^p \in K^p \subseteq F \subseteq L$ . 由题设,  $\tilde{D}(\alpha^p) = 0$ . 于是由 4.7.6,  $\tilde{D}$  可以开拓为  $L(\alpha)$  的一个导子. 这与  $(L, \tilde{D})$  的极大性矛盾. 于是  $L = K$ ,  $\tilde{D} : K \rightarrow K$  是  $D$  在  $K$  上的开拓.

(ii) 的后一论断与 (i) 的后一论断的证明完全类似. ■

**推论 4.7.9** 设  $K$  是域  $F$  的一个扩域,  $\alpha \in K$ .

(i) 在  $\text{char } F = 0$  的情形. 对于  $K$  的任何一个在  $F$  上的导子  $D$  都有  $D(\alpha) = 0$ , 必要且只要  $\alpha$  是  $F$  上的代数元.

(ii) 在  $\text{char } F = p > 0$  的情形. 对于  $K$  的任何一个在  $F$  上的导子  $D$  都有  $D(\alpha) = 0$ , 必要且只要  $\alpha \in K^p F$ .

**证** (i) 如果  $\alpha$  是  $F$  上的超越元, 由 4.7.8 (i), 总存在  $K$  的在  $F$  上的导子  $D$ , 使得  $D(\alpha) \neq 0$ .

反之, 设  $\alpha$  是  $F$  上的代数元. 则  $F(\alpha)$  是  $F$  的可分代数扩域. 令  $D$  是  $K$  的一个导子且  $D|_F = 0$ . 令  $D' = D|_{F(\alpha)}$ , 则  $D'$  是  $F(\alpha)$  的一个导子,  $D'|_F = 0$ .  $D'$  是  $F$  的平凡导子  $D_0$  在  $F(\alpha)$  上的开拓. 由 4.7.5 (ii),  $D_0$  在  $F(\alpha)$  上只有唯一的开拓, 而  $F(\alpha)$

的平凡导子显然是 $D_0$ 的一个开拓。所以 $D' = 0$ ，从而 $D(\alpha) = 0$ 。

(ii) 我们有 $K^p \subseteq K^p F \subseteq K$ 。如果 $\alpha \in K^p F$ ，那么由4.7.8(ii)，存在 $K$ 在 $K^p F$ 上的导子 $D$ ，使得 $D(\alpha) \neq 0$ 。 $D$ 自然也是在 $F$ 上平凡的。

反之，因为 $K$ 的任意在 $F$ 上的导子 $D$ 都是 $F$ -线性变换。由导子的性质立即得出，对于任意 $\alpha \in K^p F$ ，都有 $D(\alpha) = 0$ 。 ■

**推论 4.7.10** 设 $F$ 是一个域。 $\alpha \in F$ 。

(i) 在 $\text{char} F = 0$ 的情形。对于 $F$ 的任意导子 $D$ 都有 $D(\alpha) = 0$ 必要且只要 $\alpha$ 在 $F$ 的素域 $F_0$ 上是代数的。

(ii) 在 $\text{char} F = p > 0$ 的情形。对于 $F$ 的任意导子 $D$ 都有 $D(\alpha) = 0$ 必要且只要 $\alpha \in F^p$ 。

**证** 令 $F_0$ 是 $F$ 素域。则 $F_0 \cong \mathbb{Q}$ ，若 $\text{char} F = 0$ ； $F_0 \cong F_p$ ，若 $\text{char} F = p > 0$ 。 $F$ 的每一个导子在 $F_0$ 上都是平凡的。

(i) 由4.7.9(i)直接得出。

(ii)  $F_0 = F_0^p \subseteq F^p$ 。所以 $F^p F_0 = F^p$ 。于是由4.7.9(ii)，就得出这里的论断(ii)。 ■

**定理 4.7.11** 设 $K$ 是域 $F$ 的一个扩域。

(i) 如果 $K/F$ 是可分代数扩张，那么 $K$ 的每一个在 $F$ 上的导子也是 $K$ 的平凡导子。

(ii) 设 $K = F(\alpha_1, \dots, \alpha_n)$ 是 $F$ 上有限生成的扩域。如果 $K$ 的每一个在 $F$ 上的导子都是 $K$ 的平凡导子，那么 $K$ 是 $F$ 的（有限次）可分代数扩域。

**证** (i) 设 $D$ 是 $K$ 的一个在 $F$ 上的导子。如果 $D \neq 0$ ，那么一定有 $\alpha \in K$ ，使得 $D(\alpha) \neq 0$ 。于是 $D|_{F(\alpha)}$ 是 $F(\alpha)$ 的一个在 $F$ 上的导子，但 $D|_{F(\alpha)} \neq 0$ 。然而 $F(\alpha)$ 是 $F$ 的可分扩域。于是由4.7.7(ii)，必须 $D|_{F(\alpha)} = 0$ 。这就导致矛盾。

(ii) 如果 $K$ 不是 $F$ 上可分代数扩域。令 $F_0 = F$ ， $F_i = F_{i-1}(\alpha_i)$ ， $1 \leq i \leq n$ ， $F_n = K$ ，那么存在一个 $m$ ， $1 \leq m \leq n$ ，使得

$K$  是  $F_m$  上的可分代数扩域但不是  $F_{m-1}$  上的可分代数扩域. 于是  $F_m/F_{m-1}$  或者是超越扩张, 或者是不可分的代数扩张. 于是由 4.7.7, 存在  $F_m$  的导子  $D \neq 0$ , 但  $D|_{F_{m-1}} = 0$ . 而  $K = F_m(\alpha_{m+1}, \dots, \alpha_n)$  是  $F_m$  上可分代数扩域. 由 4.7.5(ii),  $D$  可以逐步开拓为  $K$  的一个导子  $\tilde{D}$ ,  $\tilde{D} \neq 0$  但  $\tilde{D}$  在  $F$  上是平凡的. ■

**定理 4.7.12** 设  $K$  是域  $F$  的一个扩域.  $K$  是  $F$  上的可分扩域必要且只要  $F$  的每一个导子都可以开拓为  $K$  的一个导子.

证 当  $\text{char } F = 0$  时,  $K/F$  是可分的. 由 4.7.8,  $F$  的每一个导子都可以开拓到  $K$  上. 这时定理显然成立.

以下设  $\text{char } F = p > 0$ .

设  $K$  是  $F$  的可分扩域. 由 4.5.2(ii),  $F$  与  $K^p$  在  $F^p$  上线性无缘. 令  $\{u_i\}_{i \in I}$  是  $F$  在  $F^p$  上一个基. 则  $\{u_i\}_{i \in I}$  在  $K^p$  上线性无关. 令  $F[K^p]$  是  $K^p$  在  $F$  上所生成的子整环,  $F[K^p] \subseteq K$ . 那么

$$\begin{aligned} F[K^p] &= \{ \sum a_i \alpha_i^p \mid (\text{有限和}) \mid a_i \in F, \alpha_i \in K \} \\ &= \{ \sum u_i \alpha_i^p \mid (\text{有限和}) \mid \alpha_i \in K \}. \end{aligned}$$

而且  $\{u_i\}_{i \in I}$  作成  $K^p$  上向量空间  $F[K^p]$  的一个基. 设  $D$  是  $F$  的一个导子. 则  $D(F^p) = 0$ . 因此  $D$  是  $F^p$  上向量空间  $F$  的一个线性变换. 所以  $D$  可以开拓为  $K^p$  上向量空间  $F[K^p]$  的一个线性变换

$$D' : F[K^p] \ni \sum u_i \alpha_i^p \mapsto \sum D(u_i) \alpha_i^p \in F[K^p].$$

易证  $D'$  是  $F[K^p]$  的导子, 且  $D'(K^p) = 0$ , 于是  $D'$  可以唯一地开拓为  $F[K^p]$  的商域  $F(K^p)$  的一个导子  $D''$ . 因为  $K \supseteq F(K^p) \supseteq K^p$ , 且  $D''(K^p) = 0$ . 于是由 4.7.8,  $D''$  可以开拓到  $K$  上.

反过来, 设  $F$  的任意导子  $D$  都可以开拓到  $K$  上. 我们证明,  $K$  与  $F^{1/p}$  在  $F$  上线性无缘.

如果存在  $u_1, \dots, u_n \in K$ ,  $u_1, \dots, u_n$  在  $F$  上线性无关, 但是在  $F^{1/p}$  上线性相关, 那么有  $a_i \in F$ ,  $a_i$  不全为零 ( $1 \leq i \leq n$ ), 使得

$$\sum_{i=1}^n a_i^{1/p} u_i = 0. \text{ 于是}$$

$$(4) \quad \sum_{i=1}^n a_i u_i^p = 0.$$

可设  $n$  是  $K$  中具有上述性质的元素的最小个数, 则  $n \geq 2$ , 并且  $a_i \neq 0$  ( $1 \leq i \leq n$ ). 因此可设  $a_n = 1$ ,

令  $\bar{D}$  是  $F$  的一个导子  $D$  在  $K$  上的开拓. 对 (4) 式施行  $\bar{D}$ . 因为  $\bar{D}(u_i^p) = 0$  ( $1 \leq i \leq n$ ),  $D(1) = 0$ , 于是得到

$$\sum_{i=1}^{n-1} \bar{D}(a_i) u_i^p = 0.$$

由  $n$  的最小性得  $\bar{D}(a_i) = 0$ ,  $1 \leq i \leq n-1$ . 因为  $D$  可以是  $F$  的任意导子, 由 4.7.10(ii), 我们有  $a_i = b_i^p \in F^p$ ,  $1 \leq i \leq n$ ,  $b_n = 1$ . 于是 (4) 式化为  $\sum_{i=1}^n b_i^p u_i^p = 0 \implies \left( \sum_{i=1}^n b_i u_i \right)^p = 0$ . 从而

$$\sum_{i=1}^n b_i u_i = 0, \quad b_i \in F, b_n = 1.$$

这与  $u_1, \dots, u_n$  在  $F$  上线性无关的假设矛盾. ■

设  $K$  是域  $F$  的一个扩域. 令  $\text{Der}(K/F)$  表示一切  $K$  的在  $F$  上的导子所成的集. 设  $D, D' \in \text{Der}(K/F)$ ,  $a, b \in K$ , 我们定义

$$(D + D')(b) = D(b) + D'(b);$$

$$(aD)(b) = aD(b),$$

那么  $\text{Der}(K/F)$  作成域  $K$  上一个向量空间.

**定理 4.7.13** 设  $K = F(X_1, \dots, X_n)$  是域  $F$  上  $n$  个不定元  $X_1, \dots, X_n$  的有理分式域. 那么导子  $\partial/\partial X_1, \dots, \partial/\partial X_n$  作成  $K$  上向量空间  $\text{Der}(K/F)$  的一个基.

**证** 设  $D$  是  $K$  在  $F$  上任意一个导子.  $D(X_i) = u_i$  ( $1 \leq i \leq n$ ).

令  $D' = D - \sum_{i=1}^n u_i \partial/\partial X_i$ . 那么  $D'(X_i) = 0$ ,  $1 \leq i \leq n$ . 所以

$$D' = 0, \quad \text{从而 } D = \sum_{i=1}^n u_i \partial/\partial X_i.$$

如果  $\sum_{i=1}^n v_i \partial/\partial X_i = 0$ ,  $v_i \in K$ . 因为  $\partial X_j/\partial X_i = \delta_{ij}$ , 这里

$\delta_{ij} = 1$ , 若  $i = j$ ,  $\delta_{ij} = 0$ , 若  $i \neq j$ . 于是  $v_j = \sum_{i=1}^n v_i (\partial X_j / \partial X_i)$   
 $= 0, 1 \leq j \leq n$ , 所以  $\partial / \partial X_1, \dots, \partial / \partial X_n$  在  $K$  上线性无关, 因而  
 作成  $\text{Der}(K/F)$  的一个基. ■

设  $F$  是一个特征为  $p > 0$  的域,  $K$  是  $F$  的一个扩域. 令  $L = K^p F$ .  $K$  的一个子集  $S$  说是在  $F$  上  $p$ -无关的, 如果对于  $S$  的任意有限个互不相同的元素  $s_1, \dots, s_n$  来说, 都有  $[L(s_1, \dots, s_n) : L] = p^n$ .

$K$  的一个在  $F$  上  $p$ -无关的子集  $S$  说是极大的, 如果不存在  $K$  的在  $F$  上  $p$ -无关的子集  $T$ , 使得  $T \supsetneq S$ .  $K$  在  $F$  上一个极大的  $p$ -无关子集叫做  $K$  在  $F$  上的一个  $p$ -基.

显然, 如果  $S^*$  是  $K$  在  $F$  上一个  $p$ -基, 那么  $K = L(S^*) = K^p F(S^*)$ .

**定理 4.7.14** 设  $K$  是域  $F$  的一个扩域,  $\text{char} F = p > 0$ .

(i) 任意给定  $K$  在  $F$  上一个  $p$ -无关的子集  $S$ , 总存在  $K$  在  $F$  上一个  $p$ -基  $S^*$ , 使得  $S^* \supseteq S$ . 特别,  $K$  在  $F$  上的  $p$ -基一定存在.

(ii) 令  $S^*$  是  $K$  在  $F$  上一个  $p$ -基,  $\Phi$  是一切  $S^*$  到  $K$  内的映射所成的集. 那么存在  $\text{Der}(K/F)$  到  $\Phi$  的一个双射  $\text{Der}(K/F) \ni D \mapsto \varphi_D \in \Phi$ , 使得  $\varphi_D(s) = D(s), \forall s \in S^*$ .

**证** (i) 利用 Zorn 引理很容易证明.

(ii) 设  $D \in \text{Der}(K/F)$ , 则  $D(K^p F) = 0$ , 所以  $\text{Der}(K/F) = \text{Der}(K/K^p F)$ . 因此, 用  $K^p F$  代替  $F$ , 并不影响定理的证明. 这样, 不失一般性, 可以假设  $K^p \subseteq F$ .

对于  $D \in \text{Der}(K/F)$ , 令  $\varphi_D : S^* \rightarrow S^*, \varphi_D(s) = D(s), \forall s \in S^*$ . 则  $\varphi_D \in \Phi$ . 所以  $D \mapsto \varphi_D$  是  $\text{Der}(K/F)$  到  $\Phi$  的一个映射. 我们证明, 这个映射是双射.

设  $\varphi \in \Phi$ . 令  $s$  是  $S^*$  的任意一个元素. 令  $S_s^* = S^* \setminus \{s\}$ . 则



$s \in F(S_s^*)$ , 而  $S^p \in F \subseteq F(S_s^*)$ . 由 4.7.8, 存在  $K = F(S^*)$  在  $F(S_s^*)$  上的导子  $D_s: K \rightarrow K$ , 使得  $D_s(s) = \varphi(s)$ .

设  $\alpha \in K = K^p F(S^*) = F(S^*)$ . 那么存在  $S = \{s_1, \dots, s_m\} \subseteq S^*$ , 使得  $\alpha \in F(s_1, \dots, s_m) = F(S)$ . 令  $D_s = \sum_{i=1}^m D_{s_i}$ . 则  $D_{s_i}(s_j) = 0$ , 若  $i \neq j$ , 因而  $D_s(s_i) = D_{s_i}(s_i) = \varphi(s_i)$ ,  $1 \leq i \leq m$ . 如果  $S' = \{s'_1, \dots, s'_r\} \subseteq S^*$ , 使得  $\alpha \in F(S')$ , 那么令  $S'' = S \cup S'$ , 则  $D_{s''}|_{F(S)} = D_s$ ,  $D_{s''}|_{F(S')} = D_{s'}$ , 于是  $D_s(\alpha) = D_{s'}(\alpha) = D_{s''}(\alpha)$ . 这样, 定义  $D: K \ni \alpha \mapsto D(\alpha) = D_s(\alpha) \in K$ , 若  $\alpha \in F(S)$ ,  $S = \{s_1, \dots, s_m\} \subseteq S^*$ . 则  $D(\alpha)$  不依赖于  $S$  的选取, 因此  $D$  是  $K$  到自身的一个映射. 易证  $D$  是  $K$  在  $F$  上一个导子, 即  $D \in \text{Der}(K/F)$ . 对于这个  $D$  来说, 我们有  $D(s) = \varphi(s)$ ,  $\forall s \in S^*$ . 所以映射  $\text{Der}(K/F) \ni D \mapsto \varphi_D \in \Phi$  是满的.

最后, 设  $D_1, D_2 \in \text{Der}(K/F)$ , 而  $D_1(s) = D_2(s)$ ,  $\forall s \in S^*$ , 那么  $D_1(\alpha) = D_2(\alpha)$ ,  $\forall \alpha \in K = F(S^*)$ , 从而  $D_1 = D_2$ . 所以上述映射  $D \mapsto \varphi_D$  是单的. ■

**推论 4.7.15** 设  $K$  是域  $F$  的一个扩域,  $\text{char } F = p > 0$ ,  $S^*$  是  $K$  在  $F$  上一个  $p$ -基. 如果  $|S^*| = n < \infty$ , 则  $\dim_K \text{Der}(K/F) = |S^*|$ .

**证** 令  $\Phi$  是一切  $S^*$  到  $K$  的映射所成的集. 对于  $\varphi, \varphi' \in \Phi$  和  $\alpha \in K$ , 定义

$$(\varphi + \varphi')(s) = \varphi(s) + \varphi'(s),$$

$$(\alpha\varphi)(s) = \alpha\varphi(s),$$

$\forall s \in S^*$ , 易证  $\Phi$  对于这样定义的运算来说作成  $K$  上一个向量空间.

$\theta: \text{Der}(K/F) \ni D \mapsto \varphi_D \in \Phi$ ,  $\varphi_D(s) = D(s)$ ,  $\forall s \in S^*$ , 是  $K$  上向量空间  $\text{Der}(K/F)$  到  $\Phi$  的线性映射. 于是由 4.7.14,  $\theta$  是  $\text{Der}(K/F)$  到  $\Phi$  的同构映射.

对于任意  $s \in S^*$ . 定义  $\sigma_s(s) = 1, \sigma_s(s') = 0$ , 若  $s' \in S^* \setminus \{s\}$ . 则  $\{\sigma_s\}_{s \in S^*}$  是  $\Phi$  的一个在  $K$  上线性无关的子集.

如果  $|S^*| < \infty$ , 那么  $\{\sigma_s\}_{s \in S^*}$  显然是向量空间  $\Phi$  在  $K$  上的一个基. 于是

$$\dim_K \text{Der}(K/F) = \dim_K \Phi = |S^*|. \quad \blacksquare$$

**定理 4.7.16** 设  $K$  是域  $F$  上一个有限生成的扩域. 以下的两个条件是等价的:

- (i)  $K$  是  $F$  上的可分扩域;
- (ii)  $\dim_K \text{Der}(K/F) = \text{tr.deg}_F K$ .

**证** (i)  $\implies$  (ii) 因为  $K/F$  是有限生成的可分扩张, 所以是可分生成的扩张. 令  $x_1, \dots, x_n$  ( $n = \text{tr.deg}_F K$ ) 是  $K/F$  的一个可分超越基,  $L = F(x_1, \dots, x_n)$ . 则  $K/L$  是可分代数扩张.  $F[x_1, \dots, x_n]$  的偏导数  $\partial/\partial x_i$  ( $1 \leq i \leq n$ ) 唯一地开拓到商域  $L = F(x_1, \dots, x_n)$  上, 是  $L$  在  $F$  上的导子, 仍以  $\partial/\partial x_i$  表示,  $\partial/\partial x_i \in \text{Der}(L/F)$ ,  $1 \leq i \leq n$ . 由 4.7.12 和 4.7.11,  $\partial/\partial x_i$  可以开拓为  $K$  的导子  $D_i, D_i \in \text{Der}(K/F)$ ,  $1 \leq i \leq n$ .

设  $D \in \text{Der}(K/F)$ .  $D(x_i) = u_i$  ( $1 \leq i \leq n$ ). 令

$$D' = D - \sum_{i=1}^n u_i D_i \in \text{Der}(K/F).$$

则  $D'(x_i) = 0$  ( $1 \leq i \leq n$ ), 于是  $D'|_L = 0$ . 由 4.7.11,  $D' = 0$ .

所以  $D = \sum_{i=1}^n u_i D_i$ .

如果  $\sum_{i=1}^n v_i D_i = 0, v_i \in K$ , 因为  $D_i(x_j) = \delta_{ij}$ , 所以

$v_i = 0$  ( $1 \leq i \leq n$ ). 这样,  $D_1, \dots, D_n$  是  $\text{Der}(K/F)$  在  $K$  上一个基, 所以  $\dim_K(K/F) = \text{tr.deg}_F K$ .

(ii)  $\implies$  (i) 如果  $\text{char } F = 0$ , 那么  $K/F$  已是可分扩张. 设  $\text{char } F = p > 0$ . 假定  $n = \dim_K \text{Der}(K/F) = \text{tr.deg}_F K$ . 则

$K$  在  $F$  上的  $p$ -基含有  $n$  个元素. 设  $s_1, \dots, s_n$  是  $K$  在  $F$  上一个  $p$ -基. 令  $D_i \in \text{Der}(K/F)$ ,  $D_i(s_j) = \delta_{ij}$ . 则  $D_1, \dots, D_n$  是  $\text{Der}(K/F)$  在  $K$  上一个基. 于是任意  $D \in \text{Der}(K/F)$  可以表成  $D = \sum_{i=1}^n u_i D_i$ , 这里  $u_i = D(s_i)$ ,  $1 \leq i \leq n$ .

令  $L = F(s_1, \dots, s_n)$ . 那么对于任意  $D \in \text{Der}(K/L)$ , 都有  $u_i = D(s_i) = 0$ ,  $1 \leq i \leq n$ , 所以  $D = 0$ . 因此  $\text{Der}(K/L) = 0$ . 因为  $K$  是  $L$  上有限生成的扩域, 所以根据 4.7.11,  $K$  是  $L$  上可分代数扩域. 我们有

$$\text{tr.deg}_F L = \text{tr.deg}_F K = n.$$

所以  $s_1, \dots, s_n$  在  $F$  上代数无关. 这样,  $s_1, \dots, s_n$  是  $K$  在  $F$  上一个可分超越基, 所以  $K/F$  是可分生成的. 由 4.6.1 (i),  $K$  是  $F$  上可分扩域. ■

## 习 题

1. 设  $R$  是一个环,  $A$  是  $R$  的一个子环.  $D$  是  $A$  到  $R$  的一个导子. 证明以下的 Leibniz 公式:

$$D^k(ab) = \sum_{i=0}^k \binom{k}{i} D^i(a) D^{k-i}(b), \quad a, b \in A.$$

2. 设  $F$  是一个域,  $K$  是  $F$  的一个扩域. 对于  $D_1, D_2 \in \text{Der}(K/F)$ ,  $a \in K$ , 定义

$$[D_1, D_2](a) = D_1 D_2(a) - D_2 D_1(a).$$

(i) 证明  $[D_1, D_2] \in \text{Der}(K/F)$ , 并且满足以下的 Jacobi 恒等式: 对于  $D_1, D_2, D_3 \in \text{Der}(K/F)$ ,

$$[[D_1, D_2], D_3] + [[D_2, D_3], D_1] + [[D_3, D_1], D_2] = 0.$$

(ii) 当  $\text{char } F = p > 0$  时,  $D^p \in \text{Der}(K/F)$ .

3. 证明, 映射  $D: R \rightarrow R$  是环  $R$  的导子必要且只要  $R$  到  $R$  上  $2 \times 2$  矩阵环内的映射

$$a \mapsto \begin{pmatrix} S & D(a) \\ 0 & a \end{pmatrix}$$

是环同态单射.

4. 设  $F$  是一个特征为  $p > 0$  的域,  $K = F(\alpha)$ , 这里  $\alpha^{p^2} \in F$  但  $\alpha^p \notin F$ , 令  $E = F(\alpha^p)$ . 证明  $\{\alpha^p\}$  是  $E$  在  $F$  上一个  $p$ -无关子集, 但不是  $K$  在  $F$  上的  $p$ -无关子集.

5. 令  $F$  是一个特征为  $p > 0$  的域,  $K$  是  $F$  的一个扩域,  $B$  是  $K$  在  $F$  上一个  $p$ -基. 证明, 对于任意正整数  $k$  来说, 都有  $K = F(K^{p^k}, B)$ .

6. 设  $F$  是一个特征为  $p > 0$  的域,  $K = F(\alpha_1, \dots, \alpha_n)$ . 证明以下论断:

(i) 如果  $D_1, \dots, D_r \in \text{Der}(K/F)$  是  $\text{Der}(K/F)$  在  $K$  上的一个基, 那么  $s_1, \dots, s_r \in K$  作成  $K/F$  的一个  $p$ -基的充要条件是矩阵  $(D_i(s_j))_{i,j=1}^r$  非退化.

(ii) 如果  $s_1, \dots, s_r \in K$  是  $K/F$  的一个  $p$ -基, 那么  $D_1, \dots, D_r \in \text{Der}(K/F)$  作成  $\text{Der}(K/F)$  在  $K$  上一个基的充要条件是矩阵  $(D_i(s_j))_{i,j=1}^r$  非退化.

7. 设  $K = F(\alpha_1, \dots, \alpha_n)$  是域  $F$  的一个扩域. 证明  $K/F$  是可分代数扩张的充要条件是存在  $n$  个多项式  $f_1, \dots, f_n \in F[X_1, \dots, X_n]$ , 使得  $f_i(\alpha_1, \dots, \alpha_n) = 0$  ( $1 \leq i \leq n$ ), 且

$$\det \left( \left( \frac{\partial f_i}{\partial X_j} \right)_\alpha \right) \neq 0,$$

$$\text{这里 } \left( \frac{\partial f_i}{\partial X_j} \right)_\alpha = \frac{\partial f_i(X_1, \dots, X_n)}{\partial X_j} \bigg|_{X_k = \alpha_k (1 \leq k \leq n)}.$$

## 第五章 整 扩 张

我们已经讨论了域的扩张。在这一章里，我们将讨论一下环的扩张。环扩张是交换代数的基本内容之一，它在代数数论和代数几何中都起着重要的作用。

在这一章里，凡是说到环，都指的是有单位元的交换环。说到一个环  $R$  的子环，都理解为含有  $R$  的单位元。

### 5.1 模

设  $R$  是一个环， $M$  是一个加法 (Abel) 群。 $M$  叫做一个左  $R$ -模，如果存在一个映射

$$R \times M \ni (r, m) \longmapsto rm \in M,$$

并且下列条件被满足：

- (1)  $r(m + m') = rm + rm', \quad \forall r \in R, m, m' \in M;$
- (2)  $(r + r')m = rm + r'm; (rr')m = r(r'm), \quad \forall r, r' \in R, m \in M.$
- (3)  $1m = m, \quad \forall m \in M.$

类似地，交换乘法的次序，可以定义右  $R$ -模。由于  $R$  是交换环，当  $M$  是一个左  $R$ -模或右  $R$ -模时，我们约定， $rm = mr, \quad \forall r \in R, m \in M$ ，则  $M$  同时成为一个右  $R$ -模或左  $R$ -模。因此，以后我们不再区分左或右  $R$ -模，而统称为  $R$ -模，或者称为环  $R$  上的模。

$R$ -模  $M$  的一个子集  $N$  叫做  $M$  的一个子模，如果在同样的运算下， $N$  也作成是一个  $R$ -模。

设  $N$  是  $R$ -模的一个子模。那么商群  $M/N$  在运算

$$R \times (M/N) \ni (r, m+N) \mapsto (rm+N) \in M/N$$

之下，也作成一个  $R$ -模，称为  $M$  对  $N$  的商模。

环  $R$  本身对于环的加法和乘法来说作成一个  $R$ -模。这时子模就是  $R$  的理想。

设  $M, N$  都是  $R$ -模。映射  $\varphi: M \rightarrow N$  叫做一个  $R$ -同态，或者叫做在  $R$  上的同态，如果

- (i)  $\varphi$  是加群  $M$  到加群  $N$  的群同态；
- (ii)  $\varphi(rm) = r\varphi(m), \forall r \in R, m \in M$ .

类似地可以定义模的  $R$ -同构。

下面的定理是群和环中有关定理的自然类比。我们只把它叙述出来，而将证明留给读者。

**定理 5.1.1** 设  $R$  是一个环。

(i) 设  $M$  是一个  $R$ -模， $N$  是  $M$  的一个子模。那么加群的自然同态  $M \rightarrow M/N$  是一个  $R$ -同态。

(ii) 设  $\varphi: M \rightarrow M'$  是  $R$ -模  $M$  到  $R$ -模  $M'$  的一个  $R$ -同态。则  $\text{Ker} \varphi$  是  $M$  的一个子模。如果  $N$  是  $M$  的一个子模且  $N \subseteq \text{Ker} \varphi$ ，那么存在唯一的  $R$ -同态  $\varphi': M/N \rightarrow M'$ ，使得  $\varphi' \cdot \pi = \varphi$ ，这里  $\pi$  是自然同态  $M \rightarrow M/N$ 。

(iii) 设  $N$  和  $N'$  都是  $R$ -模  $M$  的子模。那么子加群  $N + N'$  和  $N \cap N'$  都是子模，并且

$$(N + N')/N' \cong N/(N \cap N').$$

设  $M$  是一个环  $R$  上的模， $S \subseteq M$ 。令

$$N = \sum_{s \in S} Rs = \{ \sum r_i s_i (\text{有限和}) \mid r_i \in R, s_i \in S \}.$$

则  $N$  是  $M$  的一个子模，称为由  $S$  所生成的子模， $N$  显然是  $M$  的包含  $S$  的最小子模。子模  $N$  说是有限生成的，如果  $N$  可以由  $M$  的一个有限子集生成。 $\{0\}$  是由空集  $\emptyset$  生成的。

$R$ -模  $M$  的元素  $u_1, \dots, u_n$  说是在  $R$  上线性相关，如果存在  $R$

中不全为零的元素  $r_i (1 \leq i \leq n)$ , 使得  $\sum_{i=1}^n r_i u_i = 0$ , 否则称为在

$R$  上线性无关.  $M$  的一个子集  $S$  说是在  $R$  上线性无关, 如果  $S$  的每一个非空有限子集都在  $R$  上线性无关.

设  $M$  是一个  $R$ -模, 如果  $M$  可以由一个线性无关的子集  $S$  在  $R$  上生成, 那么就称  $M$  是一个自由  $R$ -模, 而  $S$  叫做  $M$  的一个自由基.

**定理 5.1.2** 每一个域  $F$  上的模都是自由  $F$ -模.

**证** 设  $M$  是一个  $F$ -模. 令  $\mathfrak{S}$  是  $M$  的一切线性无关子集所组成的集. 易证  $\mathfrak{S}$  对于子集的包含关系来说作成一個归纳集. 由 Zorn 引理,  $\mathfrak{S}$  有一个极大元素  $B$ . 我们证明,  $B$  是  $M$  的一个自由基. 为此, 只需证明, 由  $B$  生成的子模  $N$  与  $M$  相等.

如果不然, 那么存在  $a \in M$ , 而  $a \notin N$ . 由  $B$  的极大性可知,  $B \cup \{a\}$  不再是  $M$  的线性无关子集. 于是存在  $b_1, \dots, b_n \in B$ , 使得  $a, b_1, \dots, b_n$  在  $F$  上线性相关. 因为  $F$  是域, 而  $b_1, \dots, b_n$  在  $F$  上线性无关, 所以  $a$  可以由  $b_1, \dots, b_n$  线性表示, 从而  $a \in N$ . 这与假设矛盾. ■

由以上定理的证明中可以得出以下

**推论 5.1.3** 设  $M$  是域  $F$  上一个模而  $S$  是  $M$  的一个线性无关子集. 那么存在  $M$  的一个自由基  $B$ , 使得  $B \supseteq S$ . ■

设  $M$  和  $N$  都是环  $R$  上的模. 令  $\text{Hom}(M, N)$  表示一切  $M$  到  $N$  的  $R$ -同态所成的集. 设  $\varphi, \varphi' \in \text{Hom}(M, N), r \in R$ . 我们定义  $(\varphi + \varphi')(m) = \varphi(m) + \varphi'(m); (r\varphi)(m) = r\varphi(m), \forall m \in M$ . 则  $\text{Hom}(M, N)$  对于这样定义的运算来说作成一個  $R$ -模.

$R$ -模  $M$  的一切子模所成的集  $\mathfrak{M}$  对于集的包含关系 " $\subseteq$ " 来说, 作成一個偏序集. 设  $\mathfrak{N}$  是  $\mathfrak{M}$  的一个子集.  $A \in \mathfrak{N}$  叫做  $\mathfrak{N}$  的一个极大元素, 如果不存在  $B \in \mathfrak{N}$ , 使得  $A \subsetneq B$ . 如果  $\mathfrak{N}$  的每一个非空子集都有极大元素, 那么就说,  $M$  的子模满足极大条件.

$R$ -模  $M$  说是满足升链条件, 如果对于  $M$  的任意一个子模的升链

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

来说, 都存在一个正整数  $n$ , 使得  $M_m = M_n, \forall m \geq n$ .

**定理 5.1.4** 设  $M$  是一个环  $R$  上的模.  $M$  的子模满足极大条件必要且只要  $M$  满足升链条件.

**证** 设  $M$  的子模满足极大条件. 令

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

是  $M$  的任意一个子模升链. 那么子模的集  $\{M_i | i = 1, 2, \cdots\}$  有一个极大元素  $M_n$ . 于是  $M_n = M_m, \forall m \geq n$ . 即升链条件成立.

反之, 如果  $M$  的子模不满足极大条件, 那么存在子模所成的非空集  $\mathfrak{M}$ ,  $\mathfrak{M}$  没有极大元素. 取  $M_1 \in \mathfrak{M}$ , 则存在  $M_2 \in \mathfrak{M}$ ,  $M_1 \subsetneq M_2$ . 对于  $M_2$ , 存在  $M_3 \in \mathfrak{M}$ ,  $M_2 \subsetneq M_3$ . 如此继续下去, 就得到一个子模的无限升链

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n \subsetneq \cdots.$$

## 习 题

在以下的习题里,  $R$  代表一个有单位元 1 的交换环.

1. 证明定理 5.1.1.
2. 设  $M, M'$  是  $R$ -模,  $N, N'$  分别是  $M$  和  $M'$  的子模,  $f: M \rightarrow M'$  是一个模同态, 且  $f(N) \subseteq N'$ . 那么  $f$  诱导出商模的同态  $\bar{f}: M/N \rightarrow M'/N'$ ,  $f$  是模同构必要且只要  $f(M) + N' = M'$  且  $f^{-1}(N') = N$ .
3. 设  $M$  是一个  $R$ -模,  $N$  是  $M$  的一个子模. 证明, 在  $M$  的包含  $N$  的子模所成的集与商模  $M/N$  的子模所成的集之间存在一个双射.  $M/N$  的子模都有形状  $P/N$ , 其中  $P$  是  $M$  的子模且  $P \supseteq N$ .
4. 设  $M, N, P$  都是  $R$ -模, 且  $M \supseteq P$ . 证明  $M \cap (N + P)$



$$= (M \cap N) + P.$$

5. 设  $M$  是一个  $R$ -模. 由单独一个元素  $a \in M$  所生成的  $M$  的子模叫做循环子模. 设  $\{M_i\}_{i \in I}$  是  $M$  的一个子模族. 如果  $M$  的每一个元素  $x$  都可以唯一地表成  $x = \sum_{i \in I} x_i, x_i \in M_i$ , 并且除去有限个被加项外, 其余所有的  $x_i$  都等于 0, 那么就称  $M$  是子模族  $\{M_i\}_{i \in I}$  的直和, 记作  $M = \bigoplus_{i \in I} M_i$ . 证明, 对于  $M$  来说, 下列条件等价:

(i)  $M$  是一个自由  $R$ -模;

(ii) 存在一个非空集  $X$  和一个映射  $\iota: X \longrightarrow M$ , 具有以下性质. 对于任意一个  $R$ -模  $N$  和一个映射  $\varphi: X \longrightarrow N$ , 存在唯一的  $R$ -模同态  $f: M \longrightarrow N$ , 使得  $f \circ \iota = \varphi$ .

(iii)  $M$  是一族循环子模的直和, 每一个循环子模都模同构于  $R$ .

6. 举例说明, 一个有限生成的  $R$ -模作为加群来说不一定是有限生成的.

7. 一个  $R$ -模  $M$  叫做不可约的, 如果除  $\{0\}$  和  $M$  本身以外, 不含有其它子模. 证明, 一个有限生成的  $R$ -模  $M$  如果满足升链条件, 则  $M$  可以表示成若干不可约子模的直和.

## 5.2 Noether 环

设  $R$  是一个环. 一个  $R$ -模  $M$  叫做一个 Noether 模, 如果在  $M$  中升链条件成立. 由 5.1.4, 这个条件相当于  $M$  的子模满足极大条件.

如果  $R$  本身是一个 Noether  $R$ -模, 那么就称  $R$  是一个 Noether 环.

每一个主理想环都是 Noether 环. 特别, 每一个域都是 Noether 环.

环  $R$  本身作为  $R$ -模, 它的子模就是  $R$  的理想, 因此,  $R$  是一个 Noether 环当且仅当对于理想来说, 极大条件成立; 当且仅

当对于  $R$  的任意一个理想升链

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots,$$

都存在一个正整数  $n$ , 使得  $\mathfrak{a}_m = \mathfrak{a}_n, \forall m \geq n$ .

**定理 5.2.1** 一个环  $R$  上的模  $M$  是 Noether 模, 必要且只要  $M$  的每一个子模都是有限生成的. 环  $R$  是 Noether 环必要且只要  $R$  的每一个理想都是有限生成的.

**证** 显然只需证明第一论断.

设  $M$  是一个 Noether  $R$ -模.  $N$  是  $M$  的一个子模. 考虑由  $N$  的一切有限生成的子模所成的集  $\mathfrak{N}$ . 则  $\mathfrak{N} \neq \emptyset$ , 因为  $\{0\} \in \mathfrak{N}$ . 因为  $M$  是 Noether 模, 所以  $\mathfrak{N}$  有一个极大元素  $N_0$ . 如果  $N_0 \subsetneq N$ , 那么存在  $x \in N, x \notin N_0$ . 于是  $N'_0 = N_0 + Rx$  是  $N$  的一个有限生成的子模, 且  $N_0 \subsetneq N'_0$ . 这与  $N_0$  的极大性相违. 因此  $N_0 = N$ ,  $N$  是有限生成的.

反之, 设  $M$  的每一个子模都是有限生成的. 令  $N_1 \subseteq N_2 \subseteq \cdots$  是  $M$  的任意一个子模升链. 令  $N = \bigcup_{k=1}^{\infty} N_k$ . 则  $N$  是  $M$  的一个子模, 因而是有限生成的. 设  $N = \sum_{i=1}^n Rx_i, x_i \in N (1 \leq i \leq n)$ . 则  $x_i \in N_{k_i}$ , 对某一个  $k_i$ , 令  $m = \max n_i (1 \leq i \leq r)$ . 则  $x_i \in N_m (1 \leq i \leq n)$ , 于是  $N = N_m$ . 从而对于任意  $r \geq m$ , 都有  $N_r = N_m$ . 所以  $M$  是一个 Noether 模. ■

**定理 5.2.2** 设  $M$  是一个  $R$ -模,  $N$  是  $M$  的一个子模. 则  $M$  是 Noether 模必要且只要  $N$  和  $M/N$  都是 Noether 模.

**证** 令  $\varphi: M \rightarrow M/N$  是自然同态.

设  $M$  是 Noether 模. 令  $N_1 \subseteq N_2 \subseteq \cdots (N_i \in N)$  是  $N$  的一个子模升链. 那么存在  $m$ , 使得  $N_m = N_{m+1} = \cdots$ . 所以  $N$  也是 Noether 模.

又设  $\bar{M}_1 \subseteq \bar{M}_2 \subseteq \cdots$  是  $M/N$  的一个子模升链. 令  $M_i =$

$\varphi^{-1}(\overline{M}_i)$ . 则  $M_1 \subseteq M_2 \subseteq \cdots$  是  $M$  的一个子模升链. 于是存在  $m$ , 使得  $M_m = M_{m+1} = \cdots$ . 从而  $\overline{M}_m = \overline{M}_{m+1} = \cdots$ . 所以  $M/N$  是 Noether 模.

反之, 设  $N$  和  $M/N$  都是 Noether 模. 令  $M_1 \subseteq M_2 \subseteq \cdots$  是  $M$  的一个子模升链. 则

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots$$

和

$$\varphi(M_1) \subseteq \varphi(M_2) \subseteq \cdots$$

分别是  $N$  和  $M/N$  的子模升链. 于是存在  $m$ , 使得  $M_m \cap N = M_{m+1} \cap N = \cdots$ ,  $\varphi(M_m) = \varphi(M_{m+1}) = \cdots$ . 由此得  $M_m + N = M_{m+1} + N = \cdots$ . 于是对于任意  $n \geq m$ , 有

$$\begin{aligned} M_{n+1} &= M_{n+1} \cap (M_{n+1} + N) = M_{n+1} \cap (M_n + N) \\ &= M_n \cap (M_{n+1} + N) = M_n \cap (M_n + N) = M_n. \end{aligned}$$

所以  $M_n = M_{n+1} = \cdots$ ,  $M$  是 Noether 模. ■

**定理 5.2.3** Noether 环上有限生成模是 Noether 模.

**证** 设  $R$  是一个 Noether 环,  $M$  是一个有限生成  $R$ -模,  $u_1, \cdots, u_n$  是  $M$  的一组生成元. 我们对生成元的个数作数学归纳法.

$n=0$  时是显然的. 设  $n>0$ , 并且假设对于可以由  $n-1$  个元素生成的  $R$ -模来说, 定理成立. 现在设  $N$  是  $M$  的任意一个子模.

令  $M' = \sum_{i=2}^n R u_i$  是由  $u_2, \cdots, u_n$  所生成的子模. 由归纳假设,  $M'$  是 Noether 模. 令

$$\alpha = \{a \in R \mid a u_1 \in N + M'\}.$$

则  $\alpha$  是  $R$  的一个理想, 因而是由有限个元素生成的. 设  $\alpha = (a_1, \cdots, a_s)$ . 则  $a_i u_1 = v_i + v'_i$ ,  $v_i \in N$ ,  $v'_i \in M'$  ( $1 \leq i \leq s$ ). 我们断言,

$$N = \sum_{i=1}^s R v_i + N \cap M'.$$

事实上, 若  $u = \sum_{i=1}^n b_i u_i \in N$  ( $b_i \in R$ ), 则  $b_1 \in a$ , 从而  $b_1 = \sum_{i=1}^s r_i a_i$

( $r_i \in R$ ). 于是  $u - \sum_{i=1}^s r_i v_i \in N \cap M'$ . 所以  $u \in \sum_{i=1}^s R v_i + N \cap M'$ .

这就明了上述断言.

由归纳假设,  $N \cap M'$  作为 Noether 模  $M'$  的子模, 是有限生成的. 所以  $N$  是有限生成的. 于是由 5.2.1,  $M$  是一个 Noether 模. ■

现在我们来证明以下的定理.

**定理 5.2.4** (Hilbert 基定理) 设  $R$  是一个 Noether 环,  $R[X]$  是  $R$  上一个不定元  $X$  的多项式环. 则  $R[X]$  也是 Noether 环.

**证** 假设  $R[X]$  不是 Noether 环. 那么由 5.2.1, 存在  $R[X]$  的一个理想  $a$ ,  $a$  不是有限生成的. 令  $f_1 \in a$  是一个次数最低的多项式. 假设  $f_k$  ( $k \geq 1$ ) 已经选出, 那么选取  $f_{k+1}$  是  $a \setminus (f_1, \dots, f_k)$  中一个次数最低的多项式, 这里  $(f_1, \dots, f_k)$  表示  $f_1, \dots, f_k$  所生成的  $R[X]$  的理想.

令  $a_k \in R$  是  $f_k$  的最高次项的系数,  $n_k = \deg f_k$  ( $k = 1, 2, \dots$ ). 根据  $f_k$  的取法, 我们有  $n_1 \leq n_2 \leq \dots$ . 并且

$$(a_1) \subseteq (a_1, a_2) \subseteq \dots \subseteq (a_1, \dots, a_k) \subseteq \dots$$

是  $R$  的一个理想升链. 因为  $R$  是 Noether 环, 所以存在  $k$ , 使得  $(a_1, \dots, a_k) = (a_1, \dots, a_{k+1})$ . 于是

$$a_{k+1} = \sum_{i=1}^k r_i a_i, \quad r_i \in R.$$

这样一来,

$$g = f_{k+1} - \sum_{i=1}^k r_i X^{n_{k+1} - n_i} f_i \in I \setminus (f_1, \dots, f_k),$$

并且  $\deg g < \deg f_{k+1}$ . 这与  $f_{k+1}$  的取法矛盾. ■

由这个定理我们可以得出一系列重要的推论。

**推论 5.2.5** 一个 Noether 环  $R$  上  $n$  个不定元的多项式环  $R[X_1, \dots, X_n]$  也是 Noether 环。特别，一个域  $F$  上  $n$  个不定元的多项式环  $F[X_1, \dots, X_n]$  是 Noether 环。 ■

**推论 5.2.6** 一个 Noether 环  $R$  上由有限个元素  $\alpha_1, \dots, \alpha_n$  生成的交换环  $R[\alpha_1, \dots, \alpha_n]$  是 Noether 环。

**证**  $\varphi: R[X_1, \dots, X_n] \longrightarrow R[\alpha_1, \dots, \alpha_n]$ ,  $\varphi(X_i) = \alpha_i$  ( $1 \leq i \leq n$ ) 是一个  $R$ -模同态,  $R[\alpha_1, \dots, \alpha_n] \cong R[X_1, \dots, X_n]/\text{Ker}\varphi$ . 由 5.2.2,  $R[\alpha_1, \dots, \alpha_n]$  是 Noether 环。 ■

**推论 5.2.7** 一个域  $F$  上有限生成的交换环是 Noether 环。 ■

**定理 5.2.8** 设  $A \subseteq B \subseteq C$  是环的一个序列, 并且下列三个条件被满足:

- (i)  $A$  是 Noether 环;
- (ii)  $C$  是  $A$  上有限个元素生成的环;
- (iii)  $C$  是有限生成的  $B$ -模;

那么  $B$  作为环, 是  $A$  上有限个元素生成的。

**证** 由(ii), 存在  $x_1, \dots, x_m \in C$ , 使得  $C = A[x_1, \dots, x_m]$ .

又由(iii), 存在  $y_1, \dots, y_n \in C$ , 使得  $C = \sum_{i=1}^n B y_i$ . 我们有

$$(1) \quad x_i = \sum_{j=1}^n b_{ij} y_j, \quad b_{ij} \in B, \quad 1 \leq i \leq m.$$

$$(2) \quad y_p y_q = \sum_{r=1}^n b_{pqr} y_r, \quad b_{pqr} \in B, \quad 1 \leq p, q \leq m.$$

一切  $b_{ij}$  和  $b_{pqr}$  ( $1 \leq i \leq m, 1 \leq j, p, q, r \leq n$ ) 在  $A$  上生成  $B$  的一个子环  $B_0$ .

$$A \subseteq B_0 = A[\dots, b_{ij}, \dots, \dots, b_{pqr}, \dots] \subseteq B.$$

由(i),  $A$  是 Noether 环, 所以由 5.2.5,  $B_0$  也是 Noether 环。

$C$  的任意元素  $z$  可以表成  $z = f(x_1, \dots, x_n)$  的形式,  $f \in A[X_1, \dots, X_n]$ . 把  $x_i$  的表示式(1)代入, 反复利用(2), 可知  $z \in \sum_{i=1}^n B_0 y_i$ . 所以  $C = \sum_{i=1}^n B_0 y_i$ . 因此,  $C$  是一个有限生成的  $B_0$ -模. 因为  $B_0$  是 Noether 环, 所以由 5.2.3,  $C$  是一个 Noether  $B_0$ -模.  $B$  是  $C$  的一个子  $B_0$ -模, 所以  $B$  是有限生成的  $B_0$ -模. 因此,  $B$  是  $B_0$  上由有限个元素生成的环. 又  $B_0$  是  $A$  上由有限个元素生成的环. 所以  $B$  是  $A$  上由有限个元素生成的环. ■

**定理 5.2.9** 设  $F$  是一个域,  $B = F[x_1, \dots, x_n]$  是有限个元素  $x_1, \dots, x_n$  在  $F$  上生成的环. 如果  $B$  是域, 则  $B$  是  $F$  上有限次代数扩域.

**证** 设  $B = F[x_1, \dots, x_n]$  是域, 我们证明,  $B$  是  $F$  的代数扩域, 从而是  $F$  的有限次扩域.

如果  $B/F$  不是代数域扩张, 那么适当编号, 可以假设  $x_1, \dots, x_r$  ( $r \geq 1$ ) 在  $F$  上代数无关, 而  $x_{r+1}, \dots, x_n$  在  $E = F(x_1, \dots, x_r)$  上是代数的. 于是  $B$  是  $E$  上有限次代数扩域, 从而  $B$  是有限生成的  $E$ -模. 我们有  $F \subseteq E \subseteq B$ , 于是由 5.2.8,  $E$  作为环, 是由有限个元素  $y_1, \dots, y_s$  在  $F$  上生成的:  $E = F[y_1, \dots, y_s]$ ,  $y_i \in E = F(x_1, \dots, x_r)$ , 所以

$$y_i = f_i(x_1, \dots, x_r) / g_i(x_1, \dots, x_r), \quad f_i, g_i \in F[x_1, \dots, x_r].$$

多项式环  $F[x_1, \dots, x_r]$  含有无限多个不可约多项式. 因此存在一个不可约多项式  $p = p(x_1, \dots, x_r) \in F[x_1, \dots, x_r]$ , 使得  $p$  不能整除每一个  $g_i$  ( $1 \leq i \leq s$ ).

另一方面,  $1/p \in E = F[y_1, \dots, y_s]$ . 所以

$$\frac{1}{p} = \sum a_{i_1, \dots, i_s} y_1^{i_1} \dots y_s^{i_s}, \quad a_{i_1, \dots, i_s} \in F.$$

将  $y_i = f_i/g_i$  代入上式的右端, 然后两端同乘以  $p$  和右端各项的公分母, 我们得到

$$g_1(x_1, \dots, x_r)^{k_1} \dots g_s(x_1, \dots, x_r)^{k_s} = p(x_1, \dots, x_r) h(x_1, \dots, x_r),$$

这里  $h(x_1, \dots, x_r) \in F[x_1, \dots, x_r]$ . 由于  $F[x_1, \dots, x_r]$  是唯一因式分解整环, 所以  $p$  一定整除某一个  $g_i$ . 这就导致矛盾. 这样一来, 必须  $x_1, \dots, x_r$  都是  $F$  上的代数元, 从而  $B$  是  $F$  的代数扩域. ■

由 5.2.9 立即得到以下

**推论 5.2.10** 设  $F$  是一个域,  $B = F[x_1, \dots, x_n]$  是有限个元素在  $F$  上生成的环,  $\mathfrak{m}$  是  $B$  的一个极大理想. 那么域  $B/\mathfrak{m}$  是  $F$  上的有限次代数扩域. 特别, 如果  $F$  是代数闭域, 那么  $B/\mathfrak{m} \cong F$ . ■

**注 5.2.10** 通常称为 Hilbert 零点定理的弱形式 (参看 5.8.5).

## 习 题

在以下的习题里,  $R$  代表一个有单位元的交换环.

1.  $R$  的元素  $a$  说是不可约的, 如果  $a \neq 0$  又不是可逆元素, 并且不能写成两个非可逆元素的积. 证明, 如果  $R$  是 Noether 环, 则  $R$  中每一个既非零又非可逆的元素都可以写成若干个不可约元素的乘积.

2. 令

$$\mathfrak{a} = \{ a \in R \mid a^n = 0 \text{ 对某个 } n > 0 \}$$

是  $R$  中一切幂零元素所组成的集, 则  $\mathfrak{a}$  是  $R$  的一个理想, 称为  $R$  的幂零元素根,  $R$  的一个理想  $\mathfrak{a}$  说是幂零的, 如果存在正整数  $n$  使得  $\mathfrak{a}^n = \{ 0 \}$ . 证明, 如果  $R$  是 Noether 环, 则  $R$  的幂零元素根一定是幂零理想.

3. 设  $\mathfrak{a}$  是  $R$  的一个有限生成的理想,  $N$  是  $R$ -模  $M$  的一个子模. 如果对于每一个  $a \in \mathfrak{a}$ , 都有一个正整数  $m$  (依赖于  $a$ ), 使得  $a^m M \subseteq N$ , 则存在一个正整数  $n$ , 使  $\mathfrak{a}^n M \subseteq N$ .

4. 令  $R[[X]] = \{ (a_0, a_1, a_2, \dots) \mid a_i \in R \}$  是  $R$  的元素所组成的一切无穷序列的集. 在  $R[[X]]$  中如下地定义加法和乘法:

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

$$(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots),$$

其中  $c_k = \sum_{i+j=k} a_i b_j$ , 则  $R[[X]]$  作成有一个单位元的交换环。通

过同态单射  $R \ni a \mapsto (a, 0, 0, \dots) \in R[[X]]$ ,  $R$  被嵌入  $R[[X]]$ 。

令  $X = (0, 1, 0, \dots)$ 。则  $R[[X]]$  的元素可以唯一地写成

$$\sum_{i=0}^{\infty} a_i X^i \text{ 的形式。}$$

证明, 如果  $R$  是 Noether 环, 则  $R[[X]]$  也是 Noether 环。

### 5.3 交换环的一些理想

交换环的理想论是交换代数的基本内容之一。我们不准备详细讨论这个内容。只介绍在今后讨论中要用到的一些概念。

仍设  $R$  是一个有单位元的交换环。

$R$  的一个理想  $\mathfrak{p}$  叫做一个素理想, 如果  $\mathfrak{p} \neq R$ , 并且满足以下的条件:

$$a, b \in R, ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ 或 } b \in \mathfrak{p}.$$

**定理 5.3.1** 设  $\mathfrak{p}$  是环  $R$  的一个理想, 且  $\mathfrak{p} \neq R$ 。以下四个条件是等价的:

- (i)  $\mathfrak{p}$  是一个素理想;
- (ii)  $\mathfrak{a}, \mathfrak{b}$  是  $R$  的理想, 且  $\mathfrak{a} \mathfrak{b} \subseteq \mathfrak{p} \implies \mathfrak{a} \subseteq \mathfrak{p} \text{ 或 } \mathfrak{b} \subseteq \mathfrak{p}$ ;
- (iii)  $\mathfrak{a}, \mathfrak{b}$  是  $R$  的理想, 且  $\mathfrak{a} \not\subseteq \mathfrak{p}, \mathfrak{b} \not\subseteq \mathfrak{p} \implies \mathfrak{a} \mathfrak{b} \not\subseteq \mathfrak{p}$ ;
- (iv) 剩余类环  $R/\mathfrak{p}$  是整环。

**证** (i)  $\implies$  (ii) 设  $\mathfrak{a} \not\subseteq \mathfrak{p}$ , 那么存在  $a \in \mathfrak{a}$  但  $a \notin \mathfrak{p}$ 。于是对于任意  $b \in \mathfrak{b}$  来说, 都有  $ab \in \mathfrak{p}$ , 从而  $b \in \mathfrak{p}$ 。

(ii)  $\implies$  (iii) 显然。

(iii)  $\implies$  (iv) 令  $\bar{a} = a + \mathfrak{p}$  表示在自然同态  $R \longrightarrow R/\mathfrak{p}$  之下,  $R$  的元素  $a$  在  $R/\mathfrak{p}$  中的象。如果  $\bar{a}$  是  $R/\mathfrak{p}$  的一个零因子, 则  $\bar{a} \neq \bar{0}$ , 并且存在  $b \in R$ , 使得  $b \neq \bar{0}$ , 而  $\bar{a} \bar{b} = \bar{0}$  (即  $ab \in \mathfrak{p}$ )。



令  $a = Ra + p$ ,  $b = Rb + p$ ; 则  $a, b$  都是  $R$  的理想, 且  $a \not\subseteq p$ ,  $b \not\subseteq p$ . 于是由 (iii),  $a \cap b \not\subseteq p$ . 这与  $ab \in p$  的假设矛盾. 因此  $R/p$  没有非零的零因子.

(iv)  $\implies$  (i) 显然. ■

下面的定理可以说明素理想的存在.

环  $R$  的一个非空子集  $S$  叫做一个乘法闭子集, 如果

$$a, b \in S \implies ab \in S.$$

例如,  $R$  的一切可逆元素所成的集是一个乘法闭子集.

**定理 5.3.2** 设  $S$  是环  $R$  的一个乘法闭子集.  $\mathfrak{a}$  是  $R$  的一个理想, 且  $\mathfrak{a} \cap S = \emptyset$ . 令  $\mathfrak{S}$  是  $R$  中一切与  $S$  不相交的理想所成的集. 则  $\mathfrak{S}$  对于集的包含关系来说有一个极大元素.  $\mathfrak{S}$  的每一个极大元素都是  $R$  的素理想.

**证** 容易证明,  $\mathfrak{S}$  是一个归纳集. 由 Zorn 引理,  $\mathfrak{S}$  有一个极大元素.

设  $p$  是  $\mathfrak{S}$  的一个极大元素. 如果  $a, b$  是  $R$  的理想, 且  $a \not\subseteq p$ ,  $b \not\subseteq p$ , 那么由  $p$  的极大性,  $a \cap S$  和  $b \cap S$  分别含有元素  $a$  和  $b$ . 于是  $ab \in S$ .  $ab \in ab$ , 而  $ab \notin p$ , 所以  $ab \not\subseteq p$ . 由 5.3.1 (iii),  $p$  是素理想. ■

如果  $S$  只含有可逆元素, 那么上述定理中极大元素就是  $R$  的极大理想.

现在设  $\mathfrak{a}$  是环  $R$  的一个理想.  $R$  的子集

$$\{r \in R \mid r^n \in \mathfrak{a}, \text{ 对某个 } n\}$$

叫做  $\mathfrak{a}$  的根, 记作  $\sqrt{\mathfrak{a}}$ . 显然  $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ . 容易直接证明,  $\sqrt{\mathfrak{a}}$  是  $R$  的理想. 然而由以下定理, 也可以证明  $\sqrt{\mathfrak{a}}$  是理想.

**定理 5.3.3** 设  $\mathfrak{a}$  是环  $R$  的一个理想. 那么  $\mathfrak{a}$  的根  $\sqrt{\mathfrak{a}}$  等于  $R$  的一切包含  $\mathfrak{a}$  的素理想的交.

如果  $R$  是一个 Noether 环, 则存在一个正整数  $m$ , 使得  $(\sqrt{\mathfrak{a}})^m \subseteq \mathfrak{a}$ .

证 设  $a \in \sqrt{a}$ , 而  $p$  是任意一个包含  $a$  的素理想. 则  $a^m \in a \subseteq p$  对某个  $m$ . 从而  $a \in p$ .

反之. 设  $b \in R$ , 而  $b \notin \sqrt{a}$ . 令  $S = \{b^n \mid n \geq 0\}$ . 则  $S$  是一个乘法闭子集, 且  $a \cap S = \emptyset$ . 于是由 5.3.2, 存在一个素理想  $p \supseteq a$ , 且  $p \not\ni b$ .

如果  $R$  是 Noether 环, 那么  $\sqrt{a}$  由有限个元素生成. 设  $\sqrt{a} = (a_1, \dots, a_s)$ . 则  $a_i^{n_i} \in a$ , 对某个  $n_i (1 \leq i \leq s)$ . 令

$$m = \sum_{i=1}^s n_i. \text{ 则 } (\sqrt{a})^m \subseteq a.$$

## 习 题

1. (孙子定理) 设  $R$  是一个有单位元的交换环,  $a_1, \dots, a_n$  是  $R$  的理想, 且  $a_i + a_j = R$ , 若  $i \neq j$ . 那么对于任意给定的  $b_1, \dots, b_n \in R$ , 总存在  $b \in R$ , 使得

$$b \equiv b_i \pmod{a_i}, \quad 1 \leq i \leq n.$$

如果  $c \in R$ , 使得

$$c \equiv b_i \pmod{a_i}, \quad 1 \leq i \leq n,$$

那么  $b \equiv c \pmod{a_1 \cap \dots \cap a_n}$ .

2. 设  $f(X)$  是复数域  $C$  上一个次数大于零的多项式,  $a_1, \dots, a_r \in C$  是  $f(X)$  一切两两不同的根. 证明, 存在一个没有常数项的多项式  $p(X) \in C[X]$ , 使得

$$p(X) \equiv a_i \pmod{(X - a_i)^{m_i}} \quad 1 \leq i \leq r.$$

3. 一个  $n$  阶方阵  $A$  叫做半单的. 如果它的最小多项式没有重根;  $A$  叫做幂零的, 如果存在正整数  $m$  使得  $A^m = 0$ . 证明, 对于复数域上每一个  $n$  阶方阵  $A$ , 总存在一个半单矩阵  $D$  和一个幂零矩阵  $N$ , 它们都是  $A$  的没有常数项的多项式, 使得 (i)  $A = D + N$ ; (ii)  $DN = ND$ . 满足条件 (i) 和 (ii) 的半单矩阵和幂零矩阵是由  $A$  唯一确定的 (矩阵的 Jordan 分解).

4. 设  $F$  是一个域,  $R$  是  $F$  上一个有限生成的交换环,  $\mathfrak{a}$  是  $R$  的一个理想. 令  $J(\mathfrak{a})$  表示  $R$  的一切包含  $\mathfrak{a}$  的极大理想的交. 证明.  $J(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ .

5. 令  $R$  是一个有单位元的交换环.

(i) 设  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  是素理想,  $\mathfrak{a}$  是一个理想且

$\mathfrak{a} \subseteq \bigcup_{i=1}^r \mathfrak{p}_i$ . 则  $\mathfrak{a} \subseteq \mathfrak{p}_i$  对某一个  $i$ .

(ii) 设  $\mathfrak{a}_1, \dots, \mathfrak{a}_r$  是  $R$  的理想,  $\mathfrak{p}$  是一个素理想且

$\mathfrak{p} \supseteq \bigcap_{i=1}^r \mathfrak{a}_i$ . 则  $\mathfrak{p} \supseteq \mathfrak{a}_i$  对某一个  $i$ . 如果  $\mathfrak{p} = \bigcap_{i=1}^r \mathfrak{a}_i$ , 则  $\mathfrak{p} = \mathfrak{a}_i$

对某一个  $i$ .

6. 设  $R$  是一个有单位元的交换环,  $\mathfrak{a}, \mathfrak{b}$  是  $R$  的理想. 定义

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in R \mid x\mathfrak{b} \subseteq \mathfrak{a}\}.$$

称为  $\mathfrak{a}$  与  $\mathfrak{b}$  的商. 证明:

(i)  $(\mathfrak{a} : \mathfrak{b})$  是理想;

(ii)  $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$ ;

(iii)  $(\mathfrak{a} : \mathfrak{c})\mathfrak{c} \subseteq \mathfrak{a}$ ;

(iv)  $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$ ;

(v)  $\left(\bigcap_{i \in I} \mathfrak{a}_i : \mathfrak{b}\right) = \bigcap_{i \in I} (\mathfrak{a}_i : \mathfrak{b})$ ;

(vi)  $\left(\mathfrak{a} : \sum_{i=1}^n \mathfrak{b}_i\right) = \bigcap_{i=1}^n (\mathfrak{a} : \mathfrak{b}_i)$ .

7. 证明: 一个有单位元的交换环  $R$  是 Noether 环必要且只要  $R$  的每一个素理想都是有限生成的.

## 5.4 局部化

在这一节里, 我们将介绍交换代数中一个非常有用的概念, 这就是局部化的概念.

环的局部化正是我们所熟悉的从一个整环来构造商域过程的推广。

设  $R$  是一个环.  $S$  是  $R$  的一个乘法闭子集, 并且  $0 \notin S$ . 考虑一切元素对  $(a, s)$  所成的集

$$Q = \{(a, s) \mid a \in R, s \in S\}.$$

在  $Q$  中如下地定义一个关系: 对于  $(a, s), (a', s') \in Q$ , 定义

$$(a, s) \sim (a', s') \iff \text{存在 } t \in S, \text{ 使得 } t(s'a - sa') = 0.$$

直接验证可知,  $\sim$  是  $Q$  的一个等价关系. 由此决定  $Q$  的一个分类. 令  $a/s$  表示  $(a, s)$  所在的类. 一切类所成的集记作  $S^{-1}R$ .

我们将在  $S^{-1}R$  内定义加法和乘法, 使  $S^{-1}R$  作成有一个单位元的交换环.

首先定义加法:

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'}.$$

我们证明, 这个定义不依赖于代表的选取. 设  $a_1/s_1 = a/s$ ,  $a'_1/s'_1 = a'/s'$ . 那么存在  $t, u \in S$ , 使得

$$t(sa_1 - s_1a) = 0, \quad u(s'a'_1 - s'_1a') = 0.$$

把第一个等式乘以  $us's'_1$ , 把第二个等式乘以  $tss_1$ , 然后相加, 我们得到

$$tu(s's'_1(sa_1 - s_1a) + ss_1(s'a'_1 - s'_1a')) = 0.$$

或

$$tu(ss'(s'_1a_1 + s_1a'_1) - s_1s'_1(s'a + sa')) = 0.$$

所以

$$(s'_1a + s_1a'_1, s_1s'_1) \sim (s'a + sa', ss').$$

即

$$\frac{s'_1a_1 + s_1a'_1}{s_1s'_1} = \frac{s'a + sa'}{ss'}.$$

容易验证, 这样定义的加法满足结合律和交换律. 显然有

$s' a/s' s = a/s$ . 于是

$$\frac{0}{s'} + \frac{a}{s} = \frac{s' a}{s' s} = \frac{a}{s}.$$

所以  $0/s'$  是零元. 又

$$\frac{a}{s} + \frac{-a}{s} = \frac{0}{s^2}.$$

所以  $-a/s$  是  $a/s$  的负元. 这样,  $S^{-1}A$  对于以上定义的加法来说作成一个加群.

现在定义乘法:

$$\left(\frac{a}{s}\right)\left(\frac{a'}{s'}\right) = \frac{aa'}{ss'}.$$

易证这个定义也不依赖于代表的选取, 并且这个乘法满足结合律和交换律, 加法与乘法被分配律联系着.  $s/s (s \in S)$  显然是  $S^{-1}R$  的单位元.

这样,  $S^{-1}R$  作成有一个单位元的交换环. 称为  $R$  对于  $S$  的分式环.

对于  $R$  的每一个元素  $a$ , 类  $sa/s$  不依赖于  $s \in S$  的选取. 因此

$$\psi: R \ni a \longrightarrow sa/s \in S^{-1}R$$

是  $R$  到  $S^{-1}R$  的一个映射.  $\psi$  是一个环同态, 并且把  $R$  的单位元映成  $S^{-1}R$  的单位元.  $\psi$  称为  $R$  到  $S^{-1}R$  的自然同态.

由以上构造过程可知, 如果  $R$  是一个整环,  $S = R \setminus \{0\}$ . 则  $S^{-1}R$  就是  $R$  的商域.

一般, 如果  $R$  是一个整环, 而  $S$  是  $R$  的一个乘法闭子集且  $S \ni 0$ , 那么自然同态  $\psi: R \rightarrow S^{-1}R$  是单射. 事实上, 如果  $a \in R$ , 而  $sa/s = 0/s'$ , 则  $ss'a = 0$ , 因为  $s, s' \neq 0$ , 所以  $a = 0$ . 这时我们可以把  $\psi(R)$  与  $R$  等同起来, 而把  $R$  看成  $S^{-1}R$  的一个子环.

对于  $r \in R$ ,  $a/s \in S^{-1}R$ , 定义  $r(a/s) = ra/s$ , 则  $S^{-1}R$

作成是一个  $R$ -模.

如下构成的分式环特别重要.

设  $R$  是一个环,  $\mathfrak{p}$  是  $R$  的一个素理想. 令  $S = R \setminus \mathfrak{p}$ . 由素理想的定义知  $S$  是  $R$  的一个乘法闭子集, 且  $0 \notin S$ . 这时分式环  $S^{-1}R$  叫做  $R$  对  $\mathfrak{p}$  的分式环并且记作  $R_{\mathfrak{p}}$ .

一个环  $R$  叫做一个局部环, 如果  $R$  有唯一的极大理想.

设  $R$  是一个局部环,  $\mathfrak{m}$  是  $R$  的唯一的极大理想. 如果  $a \in R$  但  $a \notin \mathfrak{m}$ , 则  $a$  是  $R$  的一个可逆元素. 因为不然的话,  $a$  生成  $R$  的一个真理想  $(a)$ . 由于  $\mathfrak{m}$  是  $R$  的唯一的极大理想, 所以  $(a) \subseteq \mathfrak{m}$ , 这就导致矛盾.

**定理 5.4.1** 设  $R$  是一个环,  $\mathfrak{p}$  是  $R$  的一个素理想.  $R$  对于  $\mathfrak{p}$  的分式环  $R_{\mathfrak{p}}$  是一个局部环.

证 令

$$\mathfrak{m} = \mathfrak{p} R_{\mathfrak{p}} = \{p/s \mid p \in \mathfrak{p}, s \in R \setminus \mathfrak{p}\}.$$

易证  $\mathfrak{m}$  是  $R_{\mathfrak{p}}$  的一个理想. 设  $\alpha$  是  $R_{\mathfrak{p}}$  的一个理想. 如果  $\alpha \not\subseteq \mathfrak{m}$ , 则  $\alpha$  必含有一个形如  $s'/s$  的元素,  $s, s' \notin \mathfrak{p}$ . 于是  $s'/s$  在  $R_{\mathfrak{p}}$  中有逆元  $s/s'$ . 所以  $\alpha = R_{\mathfrak{p}}$ . 这就证明了  $\mathfrak{m}$  是  $R_{\mathfrak{p}}$  中唯一的极大理想, 所以  $R_{\mathfrak{p}}$  是局部环. ■

从环  $R$  过渡到  $R_{\mathfrak{p}}$  的过程叫做  $R$  在  $\mathfrak{p}$  的局部化.

## 习 题

以下说到环都指的是有单位元的交换环. 环同态  $f: R \longrightarrow R'$  都要求  $R$  的单位元映成  $R'$  的单位元.

1. 设  $f: R \longrightarrow R'$  是环同态,  $S$  是  $R$  的一个乘法闭子集, 并且对于任意  $s \in S$ ,  $f(s)$  都是  $R'$  的可逆元素. 证明, 存在唯一的环同态  $\varphi: S^{-1}R \longrightarrow R'$ , 使得  $f = \varphi \circ \psi$ , 这里  $\psi: R \longrightarrow S^{-1}R$  是自然同态.

2. 设  $S$  和  $T$  是  $R$  的两个乘法闭子集,  $U$  是  $T$  在自然同态

$R \longrightarrow S^{-1}R$  之下的象, 证明, 环  $(ST)^{-1}R$  与  $U^{-1}(S^{-1}R)$  同构.

3. (i) 设  $\mathbb{Z}$  是整数环,  $p$  是一个素数,  $\mathfrak{p} = (p)$ .  $\mathbb{Z}_{\mathfrak{p}} = ?$

(ii) 设  $f \in R, f \neq 0$ , 令  $S = \{f^n \mid n > 0\}$ . 记  $S^{-1}R = R_f$ .

如果  $R = \mathbb{Z}, f \in R, f \neq 0, R_f = ?$

4. 设  $S$  是环  $R$  的一个乘法闭子集,  $\mathfrak{a}$  是  $R$  的一个理想. 令

$$S^{-1}\mathfrak{a} = \{a/s \mid a \in \mathfrak{a}, s \in S\}.$$

(i) 证明,  $S^{-1}\mathfrak{a}$  是  $S^{-1}R$  的一个理想, 称为  $\mathfrak{a}$  在  $S^{-1}R$  中的扩张.

(ii) 设  $\mathfrak{a}, \mathfrak{b}$  是  $R$  的理想. 证明

$$(a) \quad S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b};$$

$$(b) \quad S^{-1}(\mathfrak{a} \mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b});$$

$$(c) \quad S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}.$$

$$(iii) \quad S^{-1}\mathfrak{a} = S^{-1}R \iff S \cap \mathfrak{a} = \emptyset.$$

5. 设  $\mathfrak{a}$  是  $R$  的一个理想,  $S = 1 + \mathfrak{a}$ . 证明,  $S$  是  $R$  的一个乘法闭子集, 并且  $S^{-1}\mathfrak{a}$  包含在  $S^{-1}R$  的每一个极大理想内.

6. 设  $S$  是  $R$  的一个乘法闭子集.  $\psi: R \longrightarrow S^{-1}R$  是自然同态.  $\mathfrak{b}$  是  $S^{-1}R$  的一个理想, 则  $\psi^{-1}(\mathfrak{b})$  是  $R$  的一个理想, 称为  $\mathfrak{b}$  在  $R$  中的局限. 证明:

(i) 如果  $\mathfrak{a}$  是  $R$  的一个理想, 则:  $\mathfrak{a} \subseteq \psi^{-1}(S^{-1}\mathfrak{a})$ ;

(ii) 如果  $\mathfrak{b}$  是  $S^{-1}R$  的一个理想, 则

$$S^{-1}(\psi^{-1}(\mathfrak{b})) = \mathfrak{b}.$$

(iii) 如果  $\mathfrak{p}$  是  $R$  的一个素理想且  $S \cap \mathfrak{p} = \emptyset$ , 则  $S^{-1}\mathfrak{p}$  是  $S^{-1}R$  的一个素理想且  $\psi^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$ .

(iv)  $R$  中一切与  $S$  不相交的素理想所组成的集与  $S^{-1}R$  中一切素理想所组成的集之间存在双射.

7. 证明,  $R$  是局部环的充分且必要条件是对于任意  $a, b \in R$ , 若  $a + b = 1$ , 则  $a$  或  $b$  是可逆元素.

8. 证明下列条件对于  $R$  来说是等价的:

- ( i )  $R$  是一个局部环;
- ( ii )  $R$  的一切非可逆元素都含在某一个理想  $\mathfrak{m} \neq R$  内;
- ( iii )  $R$  的一切非可逆元素作成是一个理想.

9. 设  $\mathfrak{m}$  是  $R$  的一个极大理想,  $n$  是一个正整数. 证明, 剩余类环  $R/\mathfrak{m}^n$  是局部环.

10. 证明, 局部环的任意非零同态象也是局部环.

11. 设  $R$  是一个 Noether 环,  $S$  是  $R$  的一个乘法闭子集. 则  $S^{-1}R$  也是 Noether 环.

## 5.5 整扩张

设  $R$  是一个环,  $A$  是  $R$  的一个子环. 正如本章一开始就假定的那样,  $A$  含有  $R$  的单位元.

$R$  的一个元素  $x$  说是  $A$  上的整元, 或者说,  $x$  在  $A$  上是整的, 如果存在一个系数在  $A$  内且最高次项系数是 1 的非零多项式.

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X],$$

使得  $f(x) = 0$ .

一个环  $R$  上的模  $M$  说是忠实的, 如果  $a \in R$ , 使得  $aM = 0$ , 则  $a = 0$ . 因为  $R$  有单位元, 所以环  $R$  作为  $R$ -模, 是忠实的.

**定理 5.5.1** 设  $R$  是一个环,  $A$  是  $R$  的一个子环. 对于  $R$  的元素  $x$  来说, 下列四个条件是等价的:

- ( i )  $x$  在  $A$  上是整的;
- ( ii )  $A$  上由  $x$  所生成的子环  $A[x]$  是一个有限生成的  $A$ -模;
- ( iii ) 存在  $R$  的一个子环  $B$ ,  $B \ni x$  且  $B$  是有限生成的  $A$ -模.
- ( iv ) 存在一个忠实的  $A[x]$ -模  $M$ , 且  $M$  是一个有限生成的  $A$ -模.

证 (i)  $\implies$  (ii) 设



$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad (a_i \in A, 1 \leq i \leq n).$$

那么对于任意  $r \geq 0$ , 都有

$$x^{n+r} = -(a_1 x^{n+r-1} + \cdots + a_n x^r).$$

所以  $A[x] = A + Ax + \cdots + Ax^{n-1}$  是由  $1, x, \cdots, x^{n-1}$  所生成的  $A$ -模.

(ii)  $\Rightarrow$  (iii) 取  $B = A[x]$  即可.

(iii)  $\Rightarrow$  (iv) 取  $M = B$ . 则  $M$  是一个忠实  $A[x]$ -模. 又由 (iii),  $M$  是一个有限生成  $A$ -模.

(iv)  $\Rightarrow$  (i)  $M$  是一个有限生成  $A$ -模. 令  $u_1, \cdots, u_n$  是它的一组生成元. 因为  $A[x]M \subseteq M$ , 所以  $xM \subseteq M$ . 设

$$xu_i = \sum_{j=1}^n a_{ij} u_j, a_{ij} \in A, 1 \leq i \leq n,$$

那么

$$\sum_{j=1}^n (\delta_{ij} x - a_{ij}) u_j = 0, 1 \leq i \leq n,$$

这里  $\delta_{ij} = 1$ , 若  $i = j$ ,  $\delta_{ij} = 0$ , 若  $i \neq j$ . 令

$$D = \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}.$$

那么上面的方程可以写成

$$D \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

两边乘以  $D$  的伴随矩阵  $D^*$  得

$$\det D \cdot u_k = 0, 1 \leq k \leq n.$$

所以  $\det D \in A[x]$  零化  $M$ , 即  $\det D M = 0$ . 因为  $M$  是一个忠

实  $A[x]$ -模, 所以  $\det D = 0$ . 展开这个行列式就得到

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in A (1 \leq i \leq n).$$

所以  $x$  在  $A$  上是整的. ■

由这个定理可以得出一系列重要的推论.

**推论 5.5.2** 设  $x_1, \dots, x_n \in R$  在  $A$  上是整的, 那么  $A[x_1, \dots, x_n]$  是一个有限生成的  $A$ -模.

**证** 对  $n$  作数学归纳法. 记  $A_r = A[x_1, \dots, x_r]$ . 设  $A_{n-1}$  是有限生成  $A$ -模. 由 5.5.1,  $A_n = A_{n-1}[x_n]$  是有限生成  $A_{n-1}$ -模. 所以也是有限生成的  $A$ -模. ■

**推论 5.5.3**  $R$  中一切在  $A$  上的整元所组成的集是  $R$  的一个子环.

**证** 令  $C$  是  $R$  中一切在  $A$  上的整元所成的集. 设  $x, y \in C$ . 由 5.5.2,  $A[x, y]$  是有限生成的  $A$ -模.  $x-y, xy \in A[x, y]$ , 由 5.5.1 (iii),  $x-y, xy \in C$ . ■

环  $R$  中在子环  $A$  上的整元的全体所成的环  $C$  叫做  $A$  在  $R$  内的整闭包. 如果  $C = A$ , 则称  $A$  是在  $R$  中整闭的. 如果  $C = R$ , 则称  $R$  在  $A$  上是整的. 在最后情形称  $R$  为  $A$  上的整扩环.

**推论 5.5.4** 设  $x_1, \dots, x_n \in R$  是  $A$  上的整元. 则  $A[x_1, \dots, x_n]$  是  $A$  上的整扩环.

**证** 设  $x \in A[x_1, \dots, x_n]$ . 由 5.5.2 及 5.5.1 (iii),  $x$  是  $A$  上的整元. ■

**推论 5.5.5** 设  $A$  和  $B$  都是环  $R$  的子环, 且  $A \subseteq B \subseteq R$ . 如果  $B$  是  $A$  上的整扩环,  $R$  是  $B$  上的整扩环, 则  $R$  是  $A$  上的整扩环.

**证** 设  $z \in R$ . 假定

$$z^n + b_1 z^{n-1} + \cdots + b_n = 0, \quad b_i \in B (1 \leq i \leq n).$$

令  $B' = A[b_1, \dots, b_n] \subseteq B$ . 则  $z$  是  $B'$  上的整元. 所以  $B'[z]$  是有限生成的  $B'$ -模. 又由 5.5.2,  $B'$  是有限生成的  $A$ -模. 所以

$B'[z]$ 也是有限生成的  $A$ -模.  $z \in B'[z]$ . 由 5.5.1(iii),  $z$  是  $A$  上的整元. ■

**推论 5.5.6** 设  $C$  是  $A$  在  $R$  中的整闭包. 则  $C$  在  $R$  中整闭.

**证** 设  $C'$  是  $C$  在  $R$  中的整闭包. 由 5.5.5,  $C'$  在  $A$  上是整的, 所以  $C' \subseteq C$ , 从而  $C' = C$ . ■

下面我们将证明, 一个环在其子环上的整性可以推移到相应的剩余类环和分式环上去.

设  $A$  是环  $R$  的一个子环,  $\tau$  是  $R$  的一个理想. 令  $\alpha = \tau \cap A$ . 则  $\alpha$  显然是  $A$  的一个理想. 考虑自然同态  $R \longrightarrow R/\tau$ . 在这个同态之下, 对于  $a \in A$ ,

$$A/\alpha \ni a + \alpha \longmapsto a + \tau \in R/\tau$$

是同态单射, 因此可以把  $\{a + \tau \mid a \in A\} \subseteq R/\tau$  与  $A/\alpha$  等同看待. 在这个意义下, 将  $A/\alpha$  看作  $R/\tau$  的一个子环.

**定理 5.5.7** 设  $R$  是环  $A$  的一个整扩环.

(i) 设  $\tau$  是  $R$  的一个理想,  $\alpha = \tau \cap A$ . 则剩余类环  $R/\tau$  是  $A/\alpha$  上的整扩环.

(ii) 设  $S$  是  $A$  的一个乘法闭子集. 则分式环  $S^{-1}R$  是分式环  $S^{-1}A$  上的整扩环.

**证** (i) 设  $x \in R$ . 我们有

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in A \quad (1 \leq i \leq n).$$

令  $\bar{x} = x + \tau$ . 对于  $a \in A$ , 令  $\bar{a} = a + \alpha \in A/\alpha$ . 则

$$\bar{x}^n + \bar{a}_1 \bar{x}^{n-1} + \cdots + \bar{a}_n = 0, \quad \bar{a}_i \in A/\alpha \quad (1 \leq i \leq n).$$

所以  $R/\tau$  在  $A/\alpha$  上是整的.

(ii)  $S^{-1}R$  的任意元素可以表成  $x/s$  的形式, 这里  $x \in R$ ,  $s \in S$ . 由  $x$  所满足的方程得

$$(x/s)^n + (a_1/s)(x/s)^{n-1} + \cdots + a_n/s^n = 0,$$

所以  $x/s$  是  $S^{-1}A$  上的整元. ■

**定理 5.5.8** 设  $A$  是环  $R$  的一个子环,  $C$  是  $A$  在  $R$  中的整闭

包,  $S$  是  $A$  环的一个乘法闭子集. 则  $S^{-1}C$  是  $S^{-1}A$  在  $S^{-1}R$  中的整闭包.

证 由 5.5.7,  $S^{-1}C$  在  $S^{-1}A$  上是整的. 设  $r/s \in S^{-1}R$  是  $S^{-1}A$  上一个整元. 则有,

$$(r/s)^n + (a_1/s_1)(r/s)^{n-1} + \cdots + a_n/s_n = 0$$

$a_i \in A, s_i \in S (1 \leq i \leq n)$ . 令  $t = s_1 \cdots s_n \in S$ . 把上式两边同乘以  $(st)^n$  得

$$(rt)^n + a_1 s s_2 \cdots s_n (rs)^{n-1} + \cdots + a_n s_1 \cdots s_{n-1} s^n t^n = 0.$$

所以  $rt$  是  $A$  上的整元, 从而  $rt \in C$ . 所以  $r/s = rt/st \in S^{-1}C$ .

现在设  $A$  是一个整环. 如果  $A$  在它的商域内是整闭的, 那么就称  $A$  是一个整闭整环.

**定理 5.5.9** 唯一因子分解整环是整闭整环.

证 设  $A$  是一个唯一因子分解整环,  $K$  是  $A$  的商域. 设  $a/b \in K, a, b \in A, (a, b) = 1$ . 如果  $a/b$  是  $A$  上整元, 那么等式

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0, \quad a_i \in A (1 \leq i \leq n),$$

成立. 所以

$$a^n = -a_1 a^{n-1} b - \cdots - a_n b^n.$$

如果  $b$  是  $A$  的可逆元素, 则  $a/b \in A$ . 如果  $b$  不是  $A$  的可逆元素, 则存在  $A$  的一个素元  $p$ , 使得  $p \mid b$ , 从而  $p \mid a^n$ . 所以  $p \mid a$ , 这与  $(a, b) = 1$  的假设矛盾. 这样,  $K$  在  $A$  上的整元都属于  $A$ , 即  $A$  在  $K$  内是整闭的. ■

**推论 5.5.10** 整数环  $\mathbb{Z}$ , 一个域  $F$  上的  $n$  个不定元多项式环  $F[X_1, \cdots, X_n]$  都是整闭整环. ■

## 习 题

1. 设  $B$  是环  $A$  的一个整扩环,  $f: B \longrightarrow \bar{B}$  是环同态, 且  $f(1_B) = 1_{\bar{B}}$ . 则  $f(B)$  是  $f(A)$  的整扩环.

2. 设  $B$  是环  $A$  的整扩环. 则  $B[X_1, \cdots, X_n]$  是  $A[X_1, \cdots,$

$X_n]$ 的整扩环.

3. 设  $R$  是一个有单位元的交换环,  $\{A_i\}, \{B_i\}, i \in I$ , 是  $R$  的子环族, 且  $A_i \subseteq B_i \subseteq R, \forall i \in I$ . 如果  $A_i$  在  $B_i$  中整闭,  $\forall i \in I$ , 则  $\bigcap_{i \in I} A_i$  在  $\bigcap_{i \in I} B_i$  中整闭.

4. 设  $R$  是一个整环. 证明下列断言是等价的:

(i)  $R$  是整闭的;

(ii) 对于每一个素理想  $\mathfrak{p}$ ,  $R_{\mathfrak{p}}$  是整闭的;

(iii) 对于每一个极大理想  $\mathfrak{m}$ ,  $R_{\mathfrak{m}}$  是整闭的.

## 5.6 整扩张与素理想

我们将讨论一个环与其整扩环的素理想之间的一些关系. 先证明一个事实.

**定理 5.6.1** 设  $R$  是一个整环,  $A$  是  $R$  的一个子环, 并且  $R$  在  $A$  上是整的. 那么  $R$  是域必要且只要  $A$  是域.

**证** 设  $A$  是域. 我们证明,  $R$  的每一个非零元素在  $R$  中有逆元. 设  $y \in R, y \neq 0$ . 因为  $y$  是  $A$  上的整元, 所以存在  $A$  上一个次数大于零的多项式  $f(X)$ , 使  $f(y) = 0$ . 设

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$$

是以  $y$  为根的多项式中次最低的一个. 我们有

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0.$$

因为  $R$  是整环, 所以  $a_n \neq 0$ . 因此

$$y^{-1} = -a_n^{-1}(y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1}) \in R.$$

反之, 设  $R$  是域. 则  $A$  中任意非零元素  $x$  在  $R$  中有逆元  $x^{-1}$ . 因为  $x^{-1}$  是  $A$  上的整元, 所以有

$$(x^{-1})^m + a'_1 (x^{-1})^{m-1} + \cdots + a'_m = 0, \quad a'_i \in A (1 \leq i \leq m).$$

两边乘以  $x^{m-1}$ . 我们得到

$$x^{-1} = -(a'_1 + a'_2 x + \cdots + a'_m x^{m-1}) \in A. \quad \blacksquare$$

**推论 5.6.2** 设  $R$  是环  $A$  上一个整扩环,  $\mathfrak{q}$  是  $R$  的一个素理

想。令  $p = q \cap A$ 。那么  $q$  是  $R$  的极大理想必要且只要  $p$  是  $A$  的极大理想。

证  $R/q$  是整环。由 5.5.7,  $R/q$  是  $A/p$  上的整扩环。于是由 5.6.1,  $q$  是  $R$  的极大理想  $\iff R/q$  是域  $\iff A/p$  是域  $\iff p$  是  $A$  的极大理想。 ■

推论 5.6.3 设  $R$  是环  $A$  上一个整扩环,  $q_1$  和  $q_2$  都是  $R$  的素理想, 且  $q_1 \subseteq q_2$ 。如果  $q_1 \cap A = q_2 \cap A$ , 则  $q_1 = q_2$ 。

证 令  $p = q_1 \cap A = q_2 \cap A$ 。则  $p$  是  $A$  的素理想。由 5.5.7,  $R$  对  $p$  的分式环  $R_p$  是  $A$  对  $p$  的分式环  $A_p$  上的整扩环。令  $m = p A_p$ ,  $n_1 = q_1 R_p$ ,  $n_2 = q_2 R_p$ 。则  $m$  是  $A_p$  的唯一的极大理想。我们有

$$n_1 \cap A_p = n_2 \cap A_p = m.$$

由 5.6.2,  $n_1$  和  $n_2$  都是  $R$  的极大理想。但  $n_1 \subseteq n_2$ , 所以  $n_1 = n_2$ 。因此,  $q_1 = n_1 \cap R = n_2 \cap R = q_2$ 。 ■

定理 5.6.4 (位于上(Lying over)定理) 设  $R$  是环  $A$  的一个整扩环,  $p$  是  $A$  的一个素理想。那么存在  $R$  的一个素理想  $q$ , 使得  $q \cap A = p$ 。

证 由 5.5.7, 分式环  $R_p$  是分式环  $A_p$  的整扩环。下面的图显然是交换的:

$$\begin{array}{ccc} A & \xrightarrow{\psi_A} & A_p \\ \downarrow & & \downarrow \\ R & \xrightarrow{\psi_R} & R_p \end{array}$$

在这个图里, 垂直的箭头表示自然内射,  $\psi_A: A \longrightarrow A_p$ ,  $\psi_R: R \longrightarrow R_p$  是自然同态。  $\psi_R|_A = \psi_A$ 。

令  $n$  是  $R_p$  的一个极大理想,  $m = n \cap A_p$ 。由 5.6.2,  $m$  是  $A_p$  的极大理想。然而  $A_p$  是局部环, 它有唯一的极大理想

$p A_p$ . 所以  $m = p A_p$ .  $q = \psi_R^{-1}(m)$  是  $R$  的一个素理想, 而  $q \cap A = \psi_A^{-1}(n \cap A_p) = \psi_A^{-1}(n) = p A_p \cap A = p$ . ■

**定理 5.6.5 (上升(Going up)定理)** 设  $R$  是环  $A$  上一个整扩环.  $p_1 \subseteq p_2 \subseteq \cdots \subseteq p_n$  是  $A$  的一个素理想链,  $q_1 \subseteq \cdots \subseteq q_m (m < n)$  是  $R$  的一个素理想链, 且  $q_i \cap A = p_i (1 \leq i \leq m)$ . 那么存在  $R$  的一个素理想链,  $q_1 \subseteq \cdots \subseteq q_m \subseteq q_{m+1} \subseteq \cdots \subseteq q_n$ , 使得  $q_i \cap A = p_i (1 \leq i \leq n)$ .

**证** 对  $m, n$  作双重数学归纳法. 只需对  $m=1, n=2$  的情形证明即可.

设  $p_1 \subseteq p_2$ ,  $p_1, p_2$  都是  $A$  的素理想,  $q_1$  是  $R$  的素理想且  $q_1 \cap A = p_1$ . 令  $\bar{A} = A/p_1$ ,  $\bar{R} = R/q_1$ . 由 5.5.7,  $\bar{R}$  是  $\bar{A}$  的整扩环. 令  $\bar{p}_2$  是在自然同态  $A \longrightarrow \bar{A}$  之下,  $p_2$  的象, 则  $\bar{p}_2$  是  $\bar{A}$  的素理想. 由 5.6.4, 存在  $\bar{R}$  的素理想  $\bar{q}_2$ , 使得  $\bar{q}_2 \cap \bar{A} = \bar{p}_2$ . 令  $\psi: R \longrightarrow R/q_1$  是自然同态. 令  $q_2 = \psi^{-1}(\bar{q}_2)$ . 则  $q_2$  是  $R$  的素理想. 我们有  $q_1 \subseteq q_2$ ,  $q_2 \cap A = p_2$ . ■

## 习 题

1. 设  $R$  是环  $A$  的一个整扩环,  $q$  是  $R$  中位于  $A$  的素理想  $p$  之上的一个素理想 (即  $q \cap A = p$ ). 证明,  $q$  是  $R$  的极大理想必要且只要  $p$  是  $A$  的极大理想.

2. 设  $A$  是环  $R$  的一个子环.

(i) 如果  $a \neq R$  是  $R$  的一个理想, 则  $a \cap A \neq A$  且  $a \cap A$  是  $A$  的一个理想.

(ii) 如果  $q$  是  $R$  的一个素理想, 则  $q \cap A$  是  $A$  的一个素理想.

3. 设  $C$  是环  $A$  在扩环  $B$  内的整闭包,  $a$  是  $A$  的一个理想, 令  $aC = \{\sum a_i c_i \text{ (有限和)} \mid a_i \in a, c_i \in C\}$ , 则  $aC$  是  $C$  的一个理想.  $B$  的元素  $x$  说是在  $a$  上整的, 如果  $x$  满足一个形如

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

的方程,  $a_i \in \alpha$  ( $1 \leq i \leq n$ ). 证明  $B$  的所有在  $\alpha$  上整元素所成的集等于  $\sqrt{\alpha} C$ .

4. 设  $A \subseteq B$  是整环, 其中  $A$  是整闭的,  $F$  是  $A$  的商域. 又设  $\alpha \in B$  是  $A$  的一个理想  $\alpha$  上的整元素. 证明,  $\alpha$  是  $F$  上的代数元. 令  $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$  是  $\alpha$  在  $F$  上的最小多项式, 则  $a_1, \cdots, a_n \in \sqrt{\alpha}$ .

5. (下降 (Going down) 定理) 令  $A \subseteq B$  是整环, 其中  $A$  是整闭的, 而  $B$  在  $A$  上是整的. 令  $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$  是  $A$  的一个素理想链,  $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$  ( $m < n$ ) 是  $B$  的素理想链, 使得  $\mathfrak{q}_i \cap A = \mathfrak{p}_i$  ( $1 \leq i \leq m$ ). 那么链  $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$  可以延长到素理想链  $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ , 使得  $\mathfrak{q}_i \cap A = \mathfrak{p}_i$  ( $1 \leq i \leq n$ ).

## 5.7 Noether的正规化定理

**定理 5.7.1 (Noether 的正规化定理)** 设  $F$  是一个域,  $R$  是  $F$  上有限个元素  $x_1, \cdots, x_n$  生成的环, 那么存在  $y_1, \cdots, y_m \in R$  ( $m \leq n$ ), 使得以下两个条件被满足:

- (i)  $y_1, \cdots, y_m$  在  $F$  上代数无关;
- (ii)  $R$  在子整环  $F[y_1, \cdots, y_m]$  上是整的.

**证** 对  $n$  作数学归纳法.  $n=1$  时,  $R = F[x_1]$ . 如果  $x_1$  是  $F$  上的超越元, 那么就取  $y_1 = x_1$ ; 如果  $x_1$  在  $F$  上是代数元, 这时  $m=0$ .

设  $n > 1$ , 如果  $x_1, \cdots, x_n$  在  $F$  上代数无关, 则  $m=n$ ,  $y_i = x_i$  ( $1 \leq i \leq m=n$ ). 定理已成立. 现在设  $x_1, \cdots, x_n$  在  $F$  上代数相关. 于是存在  $F$  上  $n$  个不定元  $X_1, \cdots, X_n$  的多项式

$$f(X_1, \cdots, X_n) = \sum_{(i) = (i_1, \cdots, i_n)} a_{(i)} x_1^{i_1} \cdots x_n^{i_n} \neq 0,$$

使得  $f(x_1, \cdots, x_n) = 0$ .



取定一个正整数  $t$ , 使得  $t$  大于出现在  $f$  里的一切指数组  $(i) = (i_1, \dots, i_n)$  的每一个分量. 由整数的带余除法, 每一个整数  $s$  可以唯一地表成  $t$  进整数

$$s = r_1 + r_2 t + \dots + r_k t^{k-1}, \quad 0 \leq r_i < t.$$

现在令

$$z_i = x_i - x_1^{t^{i-1}}, \quad x_i = z_i + x_1^{t^{i-1}} \quad (2 \leq i \leq n)$$

代入  $f(x_1, \dots, x_n) = 0$  中, 我们有

$$\sum_{(i)} a_{(i)} x_1^{i_1} (z_2 + x_1^t)^{i_2} \dots (z_n + x_1^{t^{n-1}})^{i_n} = 0.$$

整理以后, 上式可以写成

$$(*) \quad \sum_{(i)} a_{(i)} x_1^{i_1 + i_2 t + \dots + i_n t^{n-1}} + g(x_1, z_2, \dots, z_n) = 0,$$

这里  $g(x_1, z_2, \dots, z_n)$  是一个多项式, 它的每一项至少含有某一个  $z_i$ .

根据  $t$  的取法, 如果  $(i) = (i_1, \dots, i_n) \neq (j) = (j_1, \dots, j_n)$  是  $f$  中两个不同的指数组, 则

$$i_1 + i_2 t + \dots + i_n t^{n-1} \neq j_1 + j_2 t + \dots + j_n t^{n-1}.$$

因此, 在对应于  $f$  的指数组  $(i) = (i_1, \dots, i_n)$  的正整数  $i_1 + i_2 t + \dots + i_n t^{n-1}$  中, 有唯一的最大数  $s$ . 设  $s = p_1 + p_2 t + \dots + p_n t^{n-1}$  对应于指数组  $(p) = (p_1, \dots, p_n)$ . 于是  $(*)$  可以写成

$$a x_1^s + \sum_{j < s} u_j(z_2, \dots, z_n) x_1^j = 0,$$

这里  $a = a_{(p)} \neq 0, u_j(z_2, \dots, z_n) \in F[z_2, \dots, z_n]$ . 两边乘以  $a^{-1}$  得

$$x_1^s + \sum_{j < s} a^{-1} u_j(z_2, \dots, z_n) x_1^j = 0.$$

所以  $x_1$  是  $F[z_2, \dots, z_n]$  上的整元. 又  $x_i = z_i + x_1^{t^{i-1}} \quad (2 \leq i \leq n)$ ,

所以  $x_i \quad (2 \leq i \leq n)$  也是  $F[z_2, \dots, z_n]$  上的整元. 这样,  $R = F[x_1,$

$\cdots, x_n]$  是环  $F[z_2, \cdots, z_n]$  上的整扩环.

由归纳法的假设, 存在  $y_1, \cdots, y_m \in F[z_2, \cdots, z_n]$ ,  $m \leq n-1$ , 使得  $y_1, \cdots, y_m$  在  $F$  上代数无关, 并且  $F[z_2, \cdots, z_n]$  在  $F[y_1, \cdots, y_m]$  上是整的. 于是由 5.5.5,  $R = F[x_1, \cdots, x_n]$  在  $F[y_1, \cdots, y_m]$  上是整的. 定理被证明. ■

如果域  $F$  含有无限多个元素, 那么定理 5.7.1 还可以进一步精确化.

**定理 5.7.2** 设  $F$  是一个无限域,  $R = F[x_1, \cdots, x_n]$  是一个整环. 那么存在  $y_1, \cdots, y_m \in R$  ( $m \leq n$ ), 使得下列条件被满足:

- (i)  $y_1, \cdots, y_m$  在  $F$  上代数无关;
- (ii)  $R$  在子整环  $F[y_1, \cdots, y_m]$  上是整的;
- (iii) 每一个  $y_i$  可以表成  $y_i = \sum_{j=1}^n c_{ij} x_j$  ( $c_{ij} \in F$ ) 的形式,

$1 \leq i \leq m$ .

**证** 对  $n$  作数学归纳法.  $n=1$  时定理成立. 设  $n>1$ . 如果  $x_1, \cdots, x_n$  在  $F$  上代数无关, 则取  $y_i = x_i$  ( $1 \leq i \leq m=n$ ), 这时定理自然成立. 设  $x_1, \cdots, x_n$  在  $F$  上代数相关. 于是存在  $F[X_1, \cdots, X_n]$  的非零多项式

$$f(X_1, \cdots, X_n) = \sum_{(i)} a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \neq 0,$$

使得  $f(x_1, \cdots, x_n) = 0$ . 取  $c_2, \cdots, c_n \in F$ . 令

$$z_i = x_i - c_i x_1, \quad x_i = z_i + c_i x_1, \quad 2 \leq i \leq n,$$

这里  $c_2, \cdots, c_n \in F$  以后再确定. 代入  $f(x_1, \cdots, x_n) = 0$ , 得

$$\sum_{(i)} a_{(i)} x_1^{i_1} (z_2 + c_2 x_1)^{i_2} \cdots (z_n + c_n x_1)^{i_n} = 0.$$

整理以后得

$$\sum_{(i)} a_{(i)} c_2^{i_2} \cdots c_n^{i_n} x_1^{i_1 + i_2 + \cdots + i_n} + g(x_1, z_2, \cdots, z_n) = 0,$$

这里  $g(x_1, z_2, \dots, z_n) \in F[x_1, z_2, \dots, z_n]$ , 并且每一项至少含有某一个  $z_i$ .

上面的等式左边第一项是  $x_1$  的多项式. 设其次数为  $s$ ,  $s = \max_{(i)} (i_1 + i_2 + \dots + i_n)$ . 注意到  $g(x_1, z_2, \dots, z_n)$  中,  $x_1$  的次数都小于  $s$ , 所以上式可以写成

$$a(c_2, \dots, c_n)x_1^s + \sum_{j < s} u_j(z_2, \dots, z_n)x_1^j = 0,$$

这里  $a(Y_2, \dots, Y_n)$  是  $F$  上  $n-1$  个不定元  $Y_2, \dots, Y_n$  的一个多项式:

$$(2) \quad a(Y_2, \dots, Y_n) = \sum_{k_1 + k_2 + \dots + k_n = s} b_{k_1, \dots, k_n} Y_2^{k_2} \dots Y_n^{k_n}.$$

因为  $F$  是无限域, 所以总存在  $c_2, \dots, c_n \in F$ , 使得  $a(c_2, \dots, c_n) \neq 0$ . 取定一组  $c_2, \dots, c_n \in F$ , 使得  $c = a(c_2, \dots, c_n) \neq 0$ . 以  $c^{-1}$  乘 (2) 式的两端得

$$x_1^s + \sum_{j < s} c^{-1} u_j(z_2, \dots, z_n) x_1^j = 0.$$

所以  $x_1$  是  $F[z_2, \dots, z_n]$  上的整元, 从而  $x_i = z_i + c_i x_1 (2 \leq i \leq n)$  也是  $F[z_2, \dots, z_n]$  上的整元. 因此,  $R = F[x_1, \dots, x_n]$  在  $F[z_2, \dots, z_n]$  上是整的.

由归纳法的假设, 存在  $y_1, \dots, y_m (m \leq n-1) \in F[z_2, \dots, z_n]$ , 使得 (i)  $y_1, \dots, y_m$  在  $F$  上代数无关; (ii)  $F[z_2, \dots, z_n]$  在  $F[y_1, \dots, y_m]$  上是整的; (iii)  $y_i = \sum_{j=2}^n d_{ij} z_j (d_{ij} \in F, 1 \leq i \leq m)$ . 由 5.5.5,  $R$  在  $F[y_1, \dots, y_m]$  上是整的. 由于  $z_j = x_j - c_j x_1 (2 \leq j \leq n)$ , 所以

$$y_i = \sum_{j=1}^n c_{ij} x_j, \quad c_{ij} \in F (1 \leq i \leq m).$$

定理被证明. ■

## 5.8 代数簇 Hilbert 零点定理

从历史上来看, 求一组多项式的公共零点问题是代数学的中心问题. 这个问题尚远远未能解决. 在高等代数里曾经讨论了这个问题的两个最简单的情形, 就是某一个数域上  $n$  元一次多项式组 (线性方程组) 和一元  $n$  次多项式的情形. 在这一节里, 我们将一般地讨论一组多项式的公共零点的存在问题.

设  $K$  是一个域. 为了简单起见, 在这一节里, 我们总假定  $K$  是代数闭域. 令

$$K^n = \{(x_1, \dots, x_n) \mid x_i \in K\}$$

是  $K$  上  $n$  维向量空间, 称为  $K$  上  $n$  维仿射空间.  $K^n$  中的元素叫做点. 令  $K[X_1, \dots, X_n]$  是  $K$  上  $n$  个不定元的多项式环. 为了简单起见, 我们把  $K[X_1, \dots, X_n]$  简记作  $K[X]$ , 把  $f(X_1, \dots, X_n)$  简记作  $f(X)$ , 把  $K^n$  中的向量  $(x_1, \dots, x_n)$  简记作  $(x)$ , 把  $f(X)$  在  $(x) = (x_1, \dots, x_n)$  的值  $f(x_1, \dots, x_n)$  简记作  $f(x)$ .

设  $S$  是  $K[X]$  的一个子集. 令

$$V(S) = \{(x) \in K^n \mid f(x) = 0, \forall f \in S\}.$$

$V(S)$  叫做  $K^n$  中一个仿射代数簇, 或简称为代数簇.

令  $\alpha$  是  $S$  在  $K[x]$  内所生成的理想. 那么显然有

$$V(S) = V(\alpha).$$

设  $M$  是  $K^n$  的一个子集. 令

$$I(M) = \{f \in K[X] \mid f(x) = 0, \forall (x) \in M\}.$$

那么  $I(M)$  是  $K[X]$  的一个理想.

关于运算  $V$  和  $I$ , 以下性质成立.

**定理 5.8.1** 运算  $V$  和运算  $I$  有下列性质:

(i)  $I(K^n) = (0)$ ;  $I(\emptyset) = (1) = K[X]$ .

(ii) 对于  $K^n$  的每一个子集  $M$  来说,

$$I(M) = \sqrt{I(M)}.$$

(iii) 对于每一个代数簇  $A \subseteq K^n$ , 我们有

$$V(I(A)) = A.$$

(iv) 设  $A_1, A_2$  是  $K$  上两个代数簇.

$$A_1 \subseteq A_2 \iff I(A_1) \supseteq I(A_2),$$

并且  $A_1 \subsetneq A_2 \iff I(A_1) \supsetneq I(A_2)$ .

(v) 设  $M_1, M_2$  是  $K^n$  的两个子集, 则

$$I(M_1 \cup M_2) = I(M_1) \cap I(M_2).$$

(vi) 设  $\mathfrak{a}, \mathfrak{b}$  是  $K[X]$  的两个理想. 则

$$V(\mathfrak{a} \mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

(vii) 设  $\{\mathfrak{a}_\lambda\}_{\lambda \in \Lambda}$  是  $K[X]$  的一族理想. 令

$$\sum_\lambda \mathfrak{a}_\lambda = \{ \sum_\lambda f_\lambda \text{ (有限和)} \mid f_\lambda \in \mathfrak{a}_\lambda, \lambda \in \Lambda \}$$

是  $\{\mathfrak{a}_\lambda\}_{\lambda \in \Lambda}$  所生成的理想. 则

$$V(\sum_\lambda \mathfrak{a}_\lambda) = \bigcap_\lambda V(\mathfrak{a}_\lambda).$$

(viii) 设  $\{M_\lambda\}_{\lambda \in \Lambda}$  是  $K^n$  的一族子集. 则

$$I(\bigcup_\lambda M_\lambda) = \bigcap_\lambda I(M_\lambda).$$

证 (i) 显然  $I(\emptyset) = (1) = K[X]$ . 因为  $K$  是代数闭域, 所以是无限域. 这样就有  $I(K^n) = (0)$ .

(ii) 只需证  $\sqrt{I(M)} \subseteq I(M)$ . 设  $f \in \sqrt{I(M)}$ , 则存在正整数  $m$ , 使得  $f^m \in I(M)$ . 于是  $f(x)^m = 0, \forall (x) \in M$ , 从而  $f(x) = 0, \forall (x) \in M$ . 所以  $f \in I(M)$ .

(iii) 显然  $A \subseteq V(I(A))$ , 反之, 设  $A$  是  $K[X]$  的某一个子集  $S$  的公共零点的集. 则  $S \subseteq V(I(A))$ . 于是  $A = V(S) \supseteq V(I(A))$ .

(iv) 若  $A_1 \subseteq A_2$ , 那么显然  $I(A_1) \supseteq I(A_2)$ . 反之, 若  $I(A_1) \supseteq I(A_2)$ , 那么由 (iii)  $A_1 = V(I(A_1)) \subseteq V(I(A_2)) = A_2$ . 由此很容易得出第二个论断.

(v)  $M_i \subseteq M_1 \cup M_2$ , 所以  $I(M_1 \cup M_2) \subseteq I(M_i), i = 1, 2$ . 从而  $I(M_1 \cup M_2) \subseteq I(M_1) \cap I(M_2)$ . 反之, 设  $f \in I(M_1 \cup M_2)$ .

那么存在  $(x) \in M_1 \cup M_2$ , 使得  $f(x) \neq 0$ . 于是  $f \notin I(M_1)$  或  $f \notin I(M_2)$ , 从而  $f \notin I(M_1) \cap I(M_2)$ .

(vi) 因为  $a \cdot b \subseteq a \cap b \subseteq a, b$ . 所以

$$V(a \cdot b) \supseteq V(a \cap b) \supseteq V(a) \cup V(b).$$

反之, 设  $(x) \notin V(a) \cup V(b)$ . 则  $(x) \notin V(a)$  且  $(x) \notin V(b)$ . 于是存在  $f \in a, g \in b$ , 使得  $f(x) \neq 0, g(x) \neq 0$ , 从而  $fg(x) \neq 0$ . 然而  $fg \in a \cdot b$ . 所以  $(x) \notin V(a \cdot b)$ .

(vii)  $\sum_{\lambda} a_{\lambda} \supseteq a_{\lambda}, \forall \lambda \in \Lambda$ . 所以  $V(\sum_{\lambda} a_{\lambda}) \subseteq \bigcap_{\lambda} V(a_{\lambda})$ .

反之, 设  $(x) \notin V(\sum_{\lambda} a_{\lambda})$ , 那么存在  $f \in \sum_{\lambda} a_{\lambda}$ , 使得  $f(x) \neq 0$ .

设  $f = \sum_{i=1}^s f_i, f_i \in a_{\lambda_i}, \lambda_i \in \Lambda$ . 那么至少有一个  $f_i(x) \neq 0$ . 从而  $(x) \notin a_{\lambda_i}$ , 对某一  $\lambda_i \in \Lambda$ . 所以  $(x) \notin \bigcap_{\lambda} V(a_{\lambda})$ .

(viii) 与(vii)的证明类似. ■

设  $\alpha$  是  $K[X]$  的一个理想. 如果  $\alpha = \sqrt{\alpha}$ , 那么就称  $\alpha$  是一个根理想.

令  $\mathfrak{A}$  是  $K^n$  中一切代数簇所成的集, 令  $\mathfrak{R}$  是  $K[X]$  中一切根理想所成的集. 由 5.8.1(ii) 和 (iv), 映射  $I: \mathfrak{A} \in A \longrightarrow I(A) \in \mathfrak{R}$  是一个单射, 并且反向保持包含关系. 即  $A_1 \subseteq A_2 \implies I(A_1) \supseteq I(A_2)$ . 下面我们将会看到, 这个映射也是满射.

$K^n$  中一个代数簇  $A$  说是不可约的, 如果以下条件被满足:

若  $A = A_1 \cup A_2$ , 其中  $A_1, A_2$  都是代数簇, 那么或者  $A = A_1$ , 或者  $A = A_2$ .

**定理 5.8.2**  $K^n$  中一个代数簇  $A$  是不可约的, 必要且只要  $I(A)$  是  $K[X]$  的素理想.

**证** 设  $A$  不可约,  $f_1, f_2 \in K[X]$  且  $f_1 f_2 \in I(A)$ . 令

$$V(f_i) = \{(x) \in K^n \mid f_i(x) = 0\}, i = 1, 2.$$

令  $A_i = A \cap V(f_i), i = 1, 2$ . 则由 5.8.1 (vii),  $A_1, A_2$  都是代数

簇. 因为  $f_1 f_2(x) = 0, \forall (x) \in A$ , 所以  $f_1(x) = 0$  或  $f_2(x) = 0$ . 因此  $A \subseteq V(f_1) \cup V(f_2)$ , 从而  $A = A_1 \cup A_2$ . 于是有  $A = A_1$  或  $A = A_2$ . 由此得出  $A \subseteq V(f_1)$  或  $A \subseteq V(f_2)$ . 因此  $f_1 \in I(A)$  或  $f_2 \in I(A)$ . 所以  $I(A)$  是素理想.

反之, 设  $I(A)$  是素理想. 假设存在代数簇  $A_1, A_2$ , 使得  $A = A_1 \cup A_2$ , 且  $A_2 \subsetneq A$ . 则由 5.8.1 (iv) 和 (v), 我们有  $I(A) \subsetneq I(A_2)$  且  $I(A) = I(A_1) \cap I(A_2) = I(A_1) I(A_2)$ . 于是由 5.3.1 (ii), 我们有  $I(A_1) \subseteq I(A)$ , 从而  $A_1 = A$ . 所以  $A$  是不可约的. ■

设  $A_i \subseteq K^n$  是代数簇,  $i = 1, 2, \dots$ , 并且

$$A_1 \supseteq A_2 \supseteq \dots \supseteq A_n \supseteq \dots.$$

与此相应, 有  $K[x]$  中一个理想升链

$$I(A_1) \subseteq I(A_2) \subseteq \dots \subseteq I(A_n) \subseteq \dots.$$

因为  $K[x]$  是 Noether 环, 所以存在一个正整数  $n$ , 使得  $I(A_n) = I(A_{n+1}) = \dots$ . 于是由 5.8.1 (iv), 我们有  $A_n = A_{n+1} = \dots$ . 这时我们说, 代数簇满足降链条件.

**定理 5.8.3**  $K^n$  中每一个代数簇都可以表成有限个不可约代数簇的并.

**证** 设  $A$  是一个代数簇. 如果  $A$  不可约, 那么论断自然成立. 否则  $A = A_1 \cup A'_1$ , 其中  $A_1, A'_1$  都是代数簇, 且  $A_1 \subsetneq A$ ,  $A'_1 \subsetneq A$ . 如果  $A_1$  与  $A'_1$  中至少有一个不能表成有限个不可约代数簇的并, 比方说,  $A_1$  不能表成有限个不可约代数簇的并, 那么对  $A_1$  作同样的讨论, 就存在一个代数簇  $A_2 \subsetneq A_1$ , 并且  $A_2$  不能表成有限个不可约代数簇的并. 如此继续下去. 于是就得到代数簇的一个无限降链

$$A \supsetneq A_1 \supsetneq A_2 \supsetneq \dots.$$

这就导致矛盾. ■

**定理 5.8.4** 设  $A$  是一个代数簇. 如果

$$A = A_1 \cup \cdots \cup A_r = A'_1 \cup \cdots \cup A'_s,$$

其中  $A_i, A'_j$  都是不可约代数簇, 并且  $A_i \not\subseteq A_k, A'_j \not\subseteq A'_l$  若  $i \neq k, j \neq l$ . 那么  $r = s$ , 并且可以适当排列  $A'_j$  的次序, 使得  $A_i = A'_i, 1 \leq i \leq r = s$ .

证 首先注意以下事实, 设  $A$  是一个不可约代数簇. 如果

$$A \subseteq A_1 \cup \cdots \cup A_s,$$

其中  $A_i$  是不可约代数簇 ( $1 \leq i \leq s$ ), 那么必有某一个  $j$  ( $1 \leq j \leq s$ ), 使得  $A \subseteq A_j$ .

事实上, 我们有  $A = \bigcup_{i=1}^s (A \cup A_i)$ . 因为  $A$  不可约, 所以存在一个  $j$  ( $1 \leq j \leq s$ ), 使得  $A = A \cup A_j$ . 从而  $A \subseteq A_j$ .

现在设  $A_1 \cup \cdots \cup A_r = A'_1 \cup \cdots \cup A'_s$ ,  $A_i, A'_j$  都是不可约代数簇 ( $1 \leq i \leq r, 1 \leq j \leq s$ ). 则

$$A_1 \subseteq A'_1 \cup \cdots \cup A'_s.$$

于是由上面所证的事实, 可设  $A_1 \subseteq A'_1$ . 又因为

$$A'_1 \subseteq A_1 \cup \cdots \cup A_r,$$

所以存在某一个  $i$ , 使得  $A'_1 \subseteq A_i$ . 根据题设的条件, 必须  $i = 1$ , 从而  $A_1 = A'_1$ . 这样, 对  $r$  作数学归纳法, 就证明了这个定理. ■

现在我们证明 Hilbert 零点定理, 它是多项式组的零点存在定理.

**定理 5.8.5 (零点定理)** 设  $K$  是一个代数闭域,  $K[X]$  是  $K$  上  $n$  个不定元的多项式环,  $\alpha$  是  $K[X]$  的一个理想. 如果  $\alpha \neq K[X]$ , 则  $V(\alpha) \neq \emptyset$ .

证 因为  $\alpha \neq K[X]$ , 所以存在  $K[X]$  的一个极大理想  $m \supseteq \alpha$ . 于是  $B = K[X]/m$  是一个域. 令  $x_i$  是  $X_i$  所在的剩余类 ( $1 \leq i \leq n$ ). 于是由 5.2.9,  $B$  是  $K$  上的代数扩域. 因为  $K$  是代数闭域, 所以  $B = K$ . 于是  $(x_1, \cdots, x_n) \in K^n$  是  $m$  中多项式的一个公共零点, 因而  $(x_1, \cdots, x_n) \in V(m) \subseteq V(\alpha)$ . ■



由这个定理, 可以得出以下推论.

**推论 5.8.6** 设  $K$  是一个代数闭域.  $K$  上一个代数方程组

$$f_i(X_1, \dots, X_n) = 0, \quad f_i \in K[X] (1 \leq i \leq m),$$

在  $K^n$  中有解必要且只要  $(f_1, \dots, f_m) \neq K[X]$ .

**证** 令  $\alpha = (f_1, \dots, f_m)$ . 如果  $\alpha \neq K[X]$ , 则由零点定理有  $V(\alpha) \neq \emptyset$ , 即方程组  $f_i = 0 (1 \leq i \leq m)$  在  $K^n$  中有解.

如果  $\alpha = K[X] = (1)$ , 那么显然  $V(\alpha) = \emptyset$ . ■

**推论 5.8.7** 设  $K$  是一个代数闭域,  $\mathfrak{m}$  是  $K[X]$  的一个极大理想. 那么存在  $a_1, \dots, a_n \in K$ , 使得

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n).$$

**证** 由零点定理, 存在  $(a) = (a_1, \dots, a_n) \in V(\mathfrak{m})$ . 如果  $f \in \mathfrak{m}$ , 那么  $f(a_1, \dots, a_n) = 0$ , 因为不然的话,  $(a)$  将是  $K[X]$  的所有多项式的公共零点. 因此  $(X_1 - a_1, \dots, X_n - a_n) \subseteq \mathfrak{m}$ . 然而  $(X_1 - a_1, \dots, X_n - a_n)$  本身已是一个极大理想, 所以

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n). \quad \blacksquare$$

**定理 5.8.8** 设  $K$  是一个代数闭域,  $\alpha$  是  $K[X]$  的一个理想. 则

$$\sqrt{\alpha} = I(V(\alpha)).$$

**证** 对于  $K[X]$  的任意理想  $\alpha$  来说都有  $\sqrt{\alpha} \subseteq I(V(\alpha))$ . 现在设  $f \in I(V(\alpha))$ . 我们借助于所谓“Rabinovich 的巧思”来证明  $f \in \sqrt{\alpha}$ .

在  $K[X_1, \dots, X_n]$  上添加一个新的不相关不定元  $T$ . 在多项式环  $K[X_1, \dots, X_n, T]$  中考虑由  $\alpha$  及  $fT - 1$  所生成的理想  $\mathfrak{b}$ . 如果  $(x_1, \dots, x_n, t) \in K^{n+1}$  是  $\mathfrak{b}$  中多项式的一个公共零点, 那么将有  $(x_1, \dots, x_n) \in V(\alpha)$ , 从而  $f(x_1, \dots, x_n)t - 1 = -1$ . 然而  $(x_1, \dots, x_n, t)$  是  $f \cdot T - 1$  的零点, 这就导致矛盾. 因此  $\mathfrak{b}$  在  $K^{n+1}$  中没有零点. 由 5.8.5,  $\mathfrak{b} = K[X_1, \dots, X_n, T]$ .

因为  $K[X_1, \dots, X_n]$  是 Noether 环, 所以  $\alpha$  是由有限个元

素  $f_1, \dots, f_s \in K[X_1, \dots, X_n]$  生成的。于是我们有

$$\sum_{i=1}^s f_i g_i + h(fT - 1) = 1,$$

这里  $g_i, h \in K[X_1, \dots, X_n, T]$ ,  $1 \leq i \leq s$ .

定义一个  $K$ -同态

$$\varphi: K[X_1, \dots, X_n, T] \longrightarrow K(X_1, \dots, X_n),$$

$$\varphi(X_i) = X_i (1 \leq i \leq n), \quad \varphi(T) = \frac{1}{f}.$$

于是在  $K(X_1, \dots, X_n)$  里, 有

$$\sum_{i=1}^s f_i \varphi(g_i) = 1,$$

这里

$$\varphi(g_i(X_1, \dots, X_n, T)) = g_i(X_1, \dots, X_n, \frac{1}{f}) = \frac{u_i}{f^{k_i}},$$

$u_i \in K[X_1, \dots, X_n]$ ,  $k_i$  是一个非负整数. 令  $k = \max_{1 \leq i \leq s} \{k_i\}$ .

则  $f^k \in (f_1, \dots, f_s) = \mathfrak{a}$ , 从而  $f \in \sqrt{\mathfrak{a}}$ . ■

**推论 5.8.9** 设  $K$  是一个代数闭域,  $\mathfrak{U}$  是  $K^n$  中一切代数簇所成的集,  $\mathfrak{V}$  是  $K[X]$  中一切根理想所成的集.  $I: \mathfrak{U} \in V \longrightarrow I(A) \in \mathfrak{V}$  是一个双射. ■

**推论 5.8.10** (i) 设  $\mathfrak{a}, \mathfrak{b}$  是  $K[X]$  的两个理想,  
 $V(\mathfrak{a}) = V(\mathfrak{b}) \iff \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$ .

(ii)  $K$  上两个  $n$  元代数方程组

$$f_i(X_1, \dots, X_n) = 0 \quad (i = 1, \dots, s),$$

和

$$g_j(X_1, \dots, X_n) = 0 \quad (j = 1, \dots, t)$$

有相同的解必要且只要对于每一个  $i, 1 \leq i \leq s$ , 都有一个正整数  $k_i$ , 使得  $f_i^{k_i} \in (g_1, \dots, g_t)$ , 同时对于每一个  $j, 1 \leq j \leq t$ , 都有一个正整数  $l_j$ , 使得  $g_j^{l_j} \in (f_1, \dots, f_s)$ .

证 (i) 是 5.8.1 (ii) 和 5.8.9 的直接结果. 在 (i) 中令  $\mathfrak{a} = (f_1, \dots, f_s)$ ,  $\mathfrak{b} = (g_1, \dots, g_t)$ , 就得到 (ii). ■

## 习 题

设  $K$  是一个代数闭域,  $K[X] = K[X_1, \dots, X_n]$  是  $K$  上  $n$  个不定元的多项式环.

1. 试举一例说明, 存在  $K[X]$  的理想  $\alpha$ , 使得

$$I(V(\alpha)) \supsetneq \alpha.$$

2.  $K[X]$  中一个多项式  $f$  在  $K^n$  中的一切零点所成的集  $V(f)$  叫做一个超曲面. 证明

(i) 对于每一个超曲面  $V(f)$  来说, 一定存在  $K^n$  中无限个点不属于  $V(f)$ .

|| (ii) 每一个代数簇  $A \subseteq K^n$ , 一定存在  $K^n$  中无限多个点不属于  $A$ .

(iii) 当  $n \geq 2$  时,  $K^n$  中每一个超曲面一定含有无限多个点.

3. 设  $V(f)$  是  $K^n$  中一个超曲面, 而

$$f = cf_1^{k_1} \cdots f_s^{k_s}, \quad c \in K[X]$$

是  $f$  被分成  $K[X]$  中不可约多项式的幂的一个分解, 其中  $f_1, \dots, f_s$  是  $K[X]$  的不可约多项式, 并且两两不相伴,  $0 \neq c \in K$ ,  $k_i > 0$  ( $1 \leq i \leq s$ ). 证明  $I(V(f))$  由乘积  $f_1 \cdots f_s$  生成.

4. 证明,  $K$  上两个不定元的多项式环  $K[X_1, X_2]$  中, 素理想只有以下三种类型:

(i)  $(0)$ ; (ii) 由一个不可约多项式  $f$  所生成的主理想  $(f)$ ; (iii) 极大理想  $(X_1 - a_1, X_2 - a_2)$ , 这里  $a_1, a_2 \in K$ .

5. 设  $\sum_{j=1}^n a_{ij}x_j = b_i$  ( $1 \leq i \leq m$ ) 是  $K$  上一个线性方程组,

$A$  和  $\bar{A}$  分别是它的系数矩阵和增广矩阵. 令  $f_i = \sum_{j=1}^n a_{ij}x_j - b_i$

$\in K[X] (1 \leq i \leq m)$ . 证明以下两个条件等价:

(i) 秩  $A < \text{秩 } \bar{A}$ ;

(ii) 存在  $c_1, \dots, c_m \in K$ , 使得  $\sum_{i=1}^m c_i f_i = 1$ .

6. 证明以下两个条件等价:

(i) 对于  $K[X]$  中每一个理想  $\mathfrak{a} \neq K[X]$  来说, 都有  $V(A) \neq \emptyset$  (Hilbert 零点定理);

(ii) 设  $B$  是  $K$  上有限生成的交换环. 如果  $B$  是域, 则  $B$  是  $K$  上有限次 (代数) 扩域 (定理 5.2.9).

## 附 录

### I. Zorn 引理

设  $A$  是一个非空集. 在  $A$  上定义了一个关系, 用符号  $\leq$  表示. 如果下列条件被满足, 就称  $A$  (对于这个关系来说) 是一个偏序集:

- 1° 自反性: 对于任意  $a \in A$  都有  $a \leq a$ ;
- 2° 传递性: 如果  $a \leq b, b \leq c$ , 则  $a \leq c$ ;
- 3° 反对称性: 如果  $a \leq b, b \leq a$ , 则  $a = b$ .

例如, 设  $M$  是一个非空集,  $A$  是  $M$  的一些子集所组成的集. 则  $A$  对于集的包含关系 " $\subseteq$ " 来说作成一个偏序集.

以下设  $A$  是一个偏序集.

$A$  的一个元素  $a$  叫做  $A$  的一个极大元素, 如果对于任意  $b \in A$  来说, 只要  $a \leq b$ , 就必然有  $a = b$ .

设  $B$  是  $A$  的一个非空子集.  $a \in A$  叫做  $B$  的一个上界, 如果对于任意  $b \in B$  来说, 都有  $b \leq a$ .

$A$  的一个子集  $C$  叫做一个链, 如果对于任意  $a, b \in C$  来说, 或者  $a \leq b$ , 或者  $b \leq a$ .

**Zorn 引理** 设  $A$  是一个偏序集. 如果  $A$  的每一个链都有一个上界, 则  $A$  含有一个极大元素.

设  $A$  是一个偏序集. 如果  $A$  的每一个链都有上界, 那么就称  $A$  是一个归纳集. Zorn 引理是说, 每一个归纳集都含有一个极大元素.

## I. 基数

设  $A, B$  是两个集。如果存在一个双射,  $A \rightarrow B$ , 那么就说  $A$  与  $B$  是对等的, 并且记作  $A \sim B$ .

集的对等显然具有自反性, 对称性和传递性。彼此对等的集组成的类叫做集的对等类。每一个集属于且只属于一个对等类。

一个集  $A$  所在的对等类叫做  $A$  的基数。  $A$  的基数用符号  $|A|$  来表示。

根据这个定义, 每一个集有唯一的基数; 两个集  $A$  与  $B$  有相同的基数必要且只要  $A \sim B$ 。

令  $I_0 = \emptyset$ 。设  $n$  是一个正整数。令  $I_n = \{1, 2, \dots, n\}$  是前  $n$  个正整数所组成的集。容易证明,  $I_m \sim I_n$  当且仅当  $m = n$ 。因此, 我们把  $I_n$  的基数  $|I_n|$  与  $n$  等同看待。

一个集  $A$  如果与  $I_n$  对等, 就说  $A$  含有  $n$  个元素。与某个  $I_n$  ( $n \geq 0$ ) 对等的集叫做有限集, 否则叫做无限集。根据以上的理解, 一个有限集  $A$  的基数  $|A|$  就是  $A$  所含元素的个数。

自然数集  $\mathbb{N} = \{1, 2, 3, \dots\}$  的基数记作  $\aleph_0$  (读作aleph零)。基数为  $\aleph_0$  的集 (即与自然集对等的集) 叫做可数集。整数集  $\mathbb{Z}$ , 有理数集  $\mathbb{Q}$  都是可数集, 而实数集  $\mathbb{R}$  则不是可数集。

设  $\alpha, \beta$  是两个基数。  $A, B$  是两个不相交的集,  $|A| = \alpha, |B| = \beta$ 。  $\alpha$  与  $\beta$  的和  $\alpha + \beta$  定义为并集  $A \cup B$  基数  $|A \cup B|$ ;  $\alpha$  与  $\beta$  的积  $\alpha\beta$  定义为集合积  $A \times B$  的基数  $|A \times B|$ 。

设  $\alpha, \beta$  是两个基数。  $A, B$  是两个集, 分别以  $\alpha, \beta$  为基数:  $|A| = \alpha, |B| = \beta$ 。  $\alpha$  说是小于或等于  $\beta$ , 记作  $\alpha \leq \beta$  (或  $\beta \geq \alpha$ ), 如果  $A$  与  $B$  的一个子集对等。  $\alpha$  说是 (严格) 小于  $\beta$ , 记作  $\alpha < \beta$  (或  $\beta > \alpha$ )。 如果  $\alpha \leq \beta$  且  $\alpha \neq \beta$ 。

容易验证, 基数的加法和乘法以及大小的定义是没有歧义的, 即不依赖于集  $A$  和  $B$  的选取。

下面是关于基数的一些基本事实。这些事实的证明都不太困难。然而我们只把它们罗列在下面而略去证明。读者可以参看有关集论的书籍(例如, Hausdorff, 集论(中译本), 科学出版社, 1960)。

1° 设  $A, B$  是两个集。如果  $|A| \leq |B|$  且  $|B| \leq |A|$ , 则  $|A| = |B|$ 。

2° 对于任意两个基数  $\alpha$  与  $\beta$  来说,

$$\alpha < \beta, \alpha = \beta, \beta < \alpha$$

三种情形必有一种且仅有一种成立。

对于基数  $\alpha, \beta, \gamma$  来说,

$$\alpha \leq \beta, \beta \leq \gamma \implies \alpha \leq \gamma.$$

3° 任意一个无限集都含有一个可数子集。因此, 对于任意一个无限基数  $\alpha$  来说, 都有  $\aleph \leq \alpha$ 。

4° 设  $\alpha$  是一个无限基数,  $\beta$  是一个基数, 且  $\beta \leq \alpha$ 。则

$$(i) \quad \alpha + \beta = \alpha; \quad (ii) \quad \alpha\beta = \alpha.$$

特别, 我们有

5°  $\alpha + \aleph = \alpha, \alpha\aleph = \alpha$ , 若  $\alpha$  无限;

$\alpha + \aleph = \aleph, \alpha\aleph = \aleph$ , 若  $\alpha$  有限。

6° 令  $A$  是一个集,  $n$  是一个正整数。  $A^n = \overbrace{A \times \cdots \times A}^n$ 。

(i) 如果  $A$  是有限集, 则  $|A^n| = |A|^n$ ;

如果  $A$  是无限集, 则  $|A^n| = |A|$ 。

$$(ii) \quad \left| \bigcup_{n \in \mathbb{N}} A^n \right| = \aleph |A|.$$

7° 设  $A$  是一个无限集。令  $F(A)$  表示  $A$  的一切有限子集所组成的集。则  $|F(A)| = |A|$ 。

# 名词索引

名词	节号	名词	节号
三 画		代数无关	
子域	1.1	元素的~	4.1
上升定理	5.6	扩域的~	4.4
上界	附	代数闭包	2.1 2.2
四 画		代数闭域	2.2
中间域	1.1	代数相关	4.1
分式环	5.4	代数簇	5.8
分圆多项式	3.4	不可约的~	5.8
分圆扩域 (张)	3.5	仿射~	5.8
分裂域 (多项式的~)	2.3	可分元素	2.7
不可分元素	2.7	可分多项式	2.5
不可分多项式	2.5	可分次数 (扩域的~)	2.8
不可分次数		可分扩域 (张)	2.7 4.5
多项式的~	2.5	可分生成的扩域	4.6
扩域的~	2.8	可分的超越基	4.7
不可分扩域 (张)	2.7	可分闭包	2.7
不可约的代数簇	5.8	可解扩域 (张)	3.9
升链条件	5.1	可解群	3.8
方程的根号解	3.10	本原元素	2.10
五 画		本原 n 次单位根	3.4
正规列	3.8	归纳集	附
正规扩域 (张)	2.1	对等 (集的~)	附
代数元	1.3	六 画	
		有限域	2.4
		有限生成的扩域	1.1
		合成域	2.1



扩域	1.1
~的次数	1.1
有限生成的~	1.1
约化次数 (多项式的~)	2.5
导子	4.7
平凡~	4.7
~的开拓	4.7
导出列	3.7

### 七 画

极大元素	附
极大条件	5.1
极大 $p$ -无关子集	4.7
局部化	5.4
局部环	5.4
完备域	2.9
位子上定理	5.6
纯不可分元素	2.7
纯不可分多项式	2.5
纯不可分扩域 (张)	4.1
纯不可分闭包	4.5

### 八 画

固定域	3.1
单扩域	1.1
单位根	3.4
单群	3.8
范	3.6
忠实模	5.5
线性无缘	4.3

### 九 画

迹	3.8
---	-----

### 十 画

素域	1.2
素理想	5.3
根理想	3.8
根号扩域	3.9
特征 (域的~)	1.2
圆的 $n$ 分域	3.5
乘法闭子集	5.3

### 十一 画

基 (域的~)	1.1
基数	附
域扩张	1.1
理想的根	5.3
添加	1.1
偏序集	附

### 十二 画

超越元	1.3
超越扩域 (张)	2.1
超越次数	4.1
超越基	4.1
最小多项式	1.3
循环扩域 (张)	3.7
链	附

十四 画			
模	5.1	$F$ -自同构群	3.1
有限生成~	5.1	Galois扩域(张)	3.1
Noether~	5.2	Galois闭包	3.1
		Galois群	3.1
十六 画		Going up定理	5.6
整元	5.5	Hilbert基定理	5.2
整扩环	5.1	Hilbert零点定理	5.8
整闭包	5.5	Luroth定理	4.2
整闭环	5.5	Lying over定理	5.6
其 它		Möbius函数	3.4
Abel扩域(张)	3.5	$n$ 次一般方程	3.11
$F$ -共轭	2.3	Noether正规化定理	5.7
$F$ -同态	2.2	Noether环	5.2
$F$ -同构	2.2	Noether模	5.2
		$p$ -无关子集	4.7
		$p$ -基	4.7
		Zorn引理	附

[ G e n e r a l   I n f o r m a t i o n ]

书名= 域论基础

作者= 郝鈞新

页数= 2 3 3

S S 号= 1 0 1 0 0 8 4 0

出版日期= 1 9 8 8 年0 2 月第1 版

前言  
目录

第一章	域的扩张
	1 . 1 子域和扩域 添加
	1 . 2 素域
	1 . 3 单扩域
第二章	代数扩张
	2 . 1 代数扩域
	2 . 2 代数闭包
	2 . 3 正规扩域 多项式的分裂域
	2 . 4 有限域
	2 . 5 可分多项式和不可分多项式
	2 . 6 共轭映射的个数
	2 . 7 可分扩域和不可分扩域
	2 . 8 纯不可分扩域 可分次数和不可分次数
	2 . 9 完备域
	2 . 1 0 本原元素定理
第三章	G a l o i s 理论
	3 . 1 G a l o i s 扩域
	3 . 2 一些例子
	3 . 3 基本定理
	3 . 4 单位根
	3 . 5 分圆扩域
	3 . 6 范和迹
	3 . 7 循环扩域
	3 . 8 关于有限群的若干结果
	3 . 9 可解扩域和根号扩域
	3 . 1 0 代数方程的根号解
	3 . 1 1 n 次一般方程
	3 . 1 2 二次、三次和四次方程
第四章	超越扩张
	4 . 1 超越基 超越次数
	4 . 2 L ü r o t h 定理
	4 . 3 线性无缘
	4 . 4 域的代数无关性
	4 . 5 可分扩张
	4 . 6 可分生成的扩域
	4 . 7 导子
第五章	整扩张
	5 . 1 模
	5 . 2 N o e t h e r 环
	5 . 3 交换环的一些理想
	5 . 4 局部化
	5 . 5 整扩张

- 5 . 6 整护张与素理想
- 5 . 7 No e t h e r 的正规化定理
- 5 . 8 代数簇 H i l b e r t 零点定理

附录  
名词索引